
CROSSTALK
July 2007
The Journal of Defense Software Engineering
Vol. 20 No. 7
ENABLING TECHNOLOGIES FOR
NET-CENTRICITY

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUL 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
CrossTalk: The Journal of Defense Software Engineering. Volume 20, Number 7, July 2007	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **OO-ALC/MASE,6022 Fir Ave,Hill AFB,UT,84056-5820**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**32**	

Enabling Technologies for Net-Centricity

ON THE COVER
Cover Design by Kent Bingham

Departments

CROSSTALK

CO-SPONSORS:
DoD-CIO *The Honorable John Grimes*
NAVAIR *Jeff Schwalb*
76 SMXG *Kevin Stamey*
309 SMXG *Randy Hill*
402 SMXG *Diane Suchan*
DHS *Joe Jarzombek*

STAFF:
MANAGING DIRECTOR *Brent Baxter*
PUBLISHER *Elizabeth Starrett*
MANAGING EDITOR *Kase Johnstun*
ASSOCIATE EDITOR *Chelene Fortier-Lozancich*
ARTICLE COORDINATOR *Nicole Kentta*
PHONE (801) 775-5555
E-MAIL crosstalk.staff@hill.af.mil
CROSSTALK ONLINE www.stsc.hill.af.mil/crosstalk

CROSSTALK, The Journal of Defense Software Engineering is co-sponsored by the Department of Defense Chief Information Office (DoD-CIO); U.S. Navy (USN); U.S. Air Force (USAF); Defense Finance and Accounting Services (DFAS); and the U.S. Department of Homeland Security (DHS). DoD-CIO co-sponsor: Assistant Secretary of Defense (Networks and Information Integration). USN co-sponsor: Naval Air Systems Command. USAF co-sponsors: Oklahoma City-Air Logistics Center (ALC) 76 Software Maintenance Group (SMXG); Ogden-ALC 309 SMXG; and Warner Robins-ALC 402 SMXG. DHS co-sponsor: National Cyber Security Division of the Office of Infrastructure Protection.

The USAF Software Technology Support Center (STSC) is the publisher of CROSSTALK, providing both editorial oversight and technical review of the journal. CROSSTALK's mission is to encourage the engineering development of software to improve the reliability, sustainability, and responsiveness of our warfighting capability.

S T S C

Subscriptions: Send correspondence concerning subscriptions and changes of address to the following address. You may e-mail us or use the form on p. 16.

517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

Article Submissions: We welcome articles of interest to the defense software community. Articles must be approved by the CROSSTALK editorial board prior to publication. Please follow the Author Guidelines, available at <www.stsc.hill.af.mil/crosstalk/xtlkguid.pdf>. CROSSTALK does not pay for submissions. Articles published in CROSSTALK remain the property of the authors and may be submitted to other publications.

Reprints: Permission to reprint or post articles must be requested from the author or the copyright holder and coordinated with CROSSTALK.

Trademarks and Endorsements: This Department of Defense (DoD) journal is an authorized publication for members of the DoD. Contents of CROSSTALK are not necessarily the official views of, or endorsed by, the U.S. government, the DoD, the co-sponsors, or the STSC. All product names referenced in this issue are trademarks of their companies.

CrossTalk Online Services: See <www.stsc.hill.af.mil/crosstalk>, call (801) 777-0857 or e-mail <stsc.webmaster@hill.af.mil>.

Back Issues Available: Please phone or e-mail us to see if back issues are available free of charge.

Delivering the Power of Information

The late Edward R. Murrow once said that *television is only lights and wires in a box unless we enable the technology with value-added information*. In the world of cyberspace, our culture must move beyond form and format to embrace change. Culture change is the only way to enable information collaboration that adds true value to the lights and wires of our systems. It is the basic price of admission to fully use, share, and capitalize on information and make the best decisions in a global environment. We can no longer operate in a traditional military mode where information is locked down to the point it cannot be accessed by those who are authorized and who legitimately need it. We must register databases and metadata so authorized users can find, use, and distribute required data rapidly and effectively.

The theme of this CROSSTALK issue focuses on the technologies that enable information sharing and that are guided by four critical goals of net-centricity: to effectively build, populate, operate, and protect the net. Building the net ensures the latest, most sophisticated equipment and technology to do what is needed in a speed-of-light information world. Populating the net ensures everyone who has information crucial to someone else can make it available quickly. Operating the net means access to existing data, and protecting the net is a continual challenge to make sure we maintain the edge over any adversary who would determine to use cyberspace against the interests of the United States.

All of these elements are crucial to successfully build an information culture that shares knowledge, flattens organizations, eliminates stovepipe mentalities, and empowers a younger generation at all ranks who are becoming the hardest working and most effective information movers. When they all come together, these elements allow more effective operations at the speed demanded in today's global information environment.

Cyberspace is one of the most dynamic and challenging environments for military operations. We must consider it in the same way as the sea, space, air, and terrestrial environments. That means assuring continuous access and finding a competitive edge to ensure we maintain a free and open environment.

The information realm is enabled by technologies we have at our fingertips. Success is often measured by the speed at which we move information and our ability to use technology to share and capitalize on information. That's why we must continue to expand a collaborative culture among people who know best how to use the technology.

In a transformational culture, the military mindset must be about breaking down information stovepipes, and we should no longer hold the belief that information is the protected ground of only one group. Maintaining a controlled-access mentality can be hazardous in a world where the need for instantaneous situational awareness and rapid response may be crucial. Breaking traditions associated with stovepiped and protected information requires us to understand that every member of the team must have access. A participant's value comes from the information supplied rather than the rank held. Every value-added participant must be able to contribute to the success of our missions and objectives. We have worked very hard to operate within the necessary chain of command structure while mining the equally necessary chain of information.

Flattening information activities helps create an environment of fostering easier access and availability as we collaborate and increase decision-making speed. Decision speed and execution is what we strive for in tackling some of the toughest challenges our nation has ever faced. Waiting for perfect information places a commander behind the power curve. In fact, perfect information after the fact is useless. To increase speed, collaborative tools must become the norm. Every team member, from airman to admiral, inputs information that becomes accessible to everyone with access to authorized systems.

It's not easy to break traditional thinking and habits. Sergeants and junior officers were accustomed to clearing information through a chain of command before providing it to the upper echelon. Meeting challenges, however, is why we are in business. That includes challenges within our own systems. This is why we must continue pushing a responsive information environment, rapidly providing our nation's senior leaders with the knowledge they need to make tough decisions. The alternative is lights and wires in a box.

General James E. Cartwright
Commander, U.S. Strategic Command

Enabling Technologies for Net-Centricity – Information on Demand

The Honorable John J. Grimes
Department of Defense Chief Information Officer

The focus of net-centric operations is to provide a more effective and efficient force that includes the warfighter, the intelligence community, and the business processes that support and enable the warfighters' success. The ability to access information, to share that information, and to collaborate with others is at the heart of net-centric operations. The ongoing transformation represents a fundamental change, a strategy that requires a cultural shift regarding how information and information technology is viewed and used.

We live in a new era. The relative predictability of the Cold War is gone. As the National Defense Strategy [1] states: *Uncertainty is the defining characteristic of today's strategic environment*. The strategy emphasizes that we will not know whom we will fight, nor when, nor where, nor how. As a military, and as a nation, we must confront uncertainty with agility. Our response to unpredictable, unanticipated, and unknown security challenges of today and tomorrow must be to ensure levels of agility never before considered and never before possible.

To support the warfighter in this changing threat environment, the Department of Defense (DoD) is transforming by leveraging the power of information. Information and the ability to access it, share it, and collaborate it with others is at the heart of net-centric operations. The recent Quadrennial Defense Review (QDR) [2], reinforced the importance of achieving net-centricity and called for 15 major information technology (IT) and command and control initiatives, and significantly increased efforts to ensure information can be trusted.

The focus of the net-centric approach and activities supports the DoD's transformation and the QDR goals: to provide a more effective and efficient force. That force is not only the warfighter, but it is also the intelligence community and the business processes that enable the warfighters' success. Regardless of time or place, the user must be able to say *I can get the information I need to perform my mission*.

Atop the particular activities and programs sits a fundamental change in philosophy: It is all about the data. To successfully implement a secure enterprise-level net-centric operations capability for the warfighter, we must move away from highly tailored programs that manipulate data and move to exposing the data in a timely fashion.

The ongoing transformation represents a fundamental change in approach – that is, a change in both what is being done and how it is being accomplished. However, underlying the new strategy is perhaps a far greater challenge. There must be a dramatic cultural shift with regard to how information is viewed and used.

Stewards, Not Owners

Today, information is typically stored in bins and silos that are walled off from anyone outside a particular community. There is not only a sense of data ownership, but also an enormous cultural reluctance to share with others outside a particular community. Additionally, existing systems cannot talk to each other without the benefit of time-consuming, highly tailored, costly, pre-engineered interfaces. The approach to information security is not much different. Everything is based on predetermined needs, despite the fact that in today's world it is not possible to anticipate what will be needed nor by whom.

There must be a complete overhaul in how information is considered. Instead of the parochial attitude that *information is power*, we must move to a culture that embraces and leverages the *power of information*. That rearrangement of words is not a subtlety but the reflection of a dramatically different culture and environment. The regulatory demands of *need to know* must be met. However, the culture must shift away from over-interpretation of the requirement and place greater emphasis on understanding who else would benefit by having the information accessible. The enterprise must make authorized information sharing a priority. The importance of *need to share* and, more importantly, *right to know* must be recognized. An authorized user, in essence, has the *right to know* information that is critical to doing his or her job. The ultimate objective is to connect people with information.

The DoD Data Strategy concentrates on realizing the principles that data must be visible, accessible, and understandable [3]. An authorized and authenticated user must be able to discover that data exists, pull it off the network, and use it. To do so requires *tagging* of all data with metadata and enterprise-wide registries to enable discovery by users. Communities of interest are forming across a wide variety of areas, including Maritime Domain Awareness, which has improved the ability to share information across the breadth of military, federal, state, local, and private organizations, increasing the security of our harbors and ports.

We must become stewards, not owners, of information.

Enterprise, Not Stovepipe

Today's data silos support a mentality in which information is, quite frankly, hidden and hoarded rather than visible and shared. Dealing with the unanticipated demands the latter. As the people, processes, and technology of the net-centric Global Information Grid (GIG) mature, the goal of sharing information must serve as the guiding vision. The challenge is to design, engineer, and create an information environment rather than focus on platforms and systems alone.

The approach, therefore, is to successfully introduce and continually evolve the GIG through enterprise-wide system engineering – not tailored stovepipes. This effort sets the path that the rest of the enterprise can easily follow by establishing enterprise-wide technical baselines, analysis capabilities, and compliance management. In short, emphasis must be placed on the whole enterprise and the foundation upon which it will support the full range of future users.

We must develop the net-centric GIG as an enterprise, not stovepipes.

Services, Not Systems

Today's world is focused on systems. That is, programs that retrieve and manipulate data are typically developed according to very specific and highly tailored requirements. Each organization or function tends to pursue its own needs. The result has been a bevy of systems that not only cannot communicate with each other but do not even use the same language. The proprietary applications currently in use are not open, not easily changed, and not transferable to other needs.

Services-Oriented Architecture (SOA) is the key to transformation in an age of shared information needs. Specifically, SOA supports an information environment built upon loosely coupled, reusable, standards-based services. It promotes data interoperability rather than application interoperability. SOA ensures providers can reuse what already exists – that is, pieces of applications and data rather than re-create them every time. Moreover, it allows new capabilities to be delivered more quickly. The practice of buying individual, highly tailored, proprietary systems must end. We must place a new focus on separating data from applications for use within and across the Enterprise Information Environment (EIE).

The second key to success is leveraging commercially managed services. The EIE will provide commonly available core services – that is, services commonly needed by a wide range of users. Services are required to access, manipulate, share, and, most importantly, collaborate data. They must be viewed as resources to manage rather than applications to own. Unnecessary duplication of services readily available in the marketplace must end. Buying *things* must be replaced with services purchased and billed based on usage. Simply put, the DoD will not develop, own, run, or install every service it might need. The Net-Centric Enterprise Services program under way at Defense Information Systems Agency (DISA) is key to how we are changing.

We must concentrate on services, not systems.

Portfolios, Not Programs

Finally, there is a fundamental change in the management and oversight of the many efforts involved in this transformation. It is a change that is understood conceptually and its importance is understood, but the actual implementation is still being sorted out. The 2006 QDR took steps to move us from threat-based acquisitions to a capability-based environment. In a world of unknown challenges and unanticipated needs and partners, focusing on capabilities is essential. The theory is on target, but the execution is tricky.

Traditionally, the acquisition environment has been viewed as a collection of programs and systems – that is, individual activities that lead to a specific product. Over time, the concept of systems of systems developed. Regardless of terminology, the emphasis was still oriented on delivering physical platforms or lines of code. There has been a tendency to create tidy packages that could more easily be managed – despite the fact that the relationship of the many packages to the warfighter's needs remained fundamentally unclear.

Net-centric operations will require bringing individual programs under umbrellas that represent actual and complete capabilities. The QDR initiated four Capability Portfolio Management (CPM) test cases. The CPMs not only pull related, integrated, and synergistic programs under a common management frame, but also consider whether or not there are duplications to mediate or legacy programs to cut. The process offers the ability to look at the whole rather than struggle to determine if there should be a connection between the parts.

In September of 2006, the Deputy Secretary of Defense (DepSecDef) signed a memo articulating the ultimate objective of the CPM test cases: *ensuring the ability to deliver a capability portfolio aligned with strategic intent*. In addition to that overall guidance on CPM, the leadership now regularly reviews progress through the DepSecDef's Advisory Working Group. The National Information Infrastructure/ Chief Information Officer (CIO) shares primary responsibility for the Joint Net-Centric Operations, and the Joint Command and Control test cases. Preliminary results from both have led to issue papers that are currently being reviewed by Program Analysis and Evaluation. The final two test cases, which the DoD also supports, are Joint Battlespace Awareness and Joint Logistics. These CPM test cases are consistent with the DoD policy on IT portfolio management. By focusing on capabilities needed, rather than programs funded, the needs of the warfighter are better met.

We must manage by portfolios, not programs.

Challenges Ahead

Much of what must be done is well understood, but many areas and needs have yet to be invented. Many challenges lie ahead.

Establishing an information sharing culture is critical; making it happen is equally critical. Cross-domain solutions are one of those challenges. Specifically, the movement of information across domains, both vertical and horizontal, must be addressed. Whether crossing organizational boundaries and moving information horizontally or maneuvering security levels and moving information vertically, the ability to leverage information throughout the national security community is essential.

Information Assurance (IA), another key area of focus in the QDR, is the basis for timely and trusted information. The threat is real. It is here, it is now, it is persistent, and it is *maturing*. Most importantly, we must change our approach. Security approaches must move from fences and patches that keep intruders out and toward data that is secure throughout its useful lifetime – secure from the start. IA is one of the most complex and important aspects of information sharing.

The *IA Component of the GIG Integrated Architecture* [4], originally released in late 2004, provides the strategy and the way ahead. It focuses on five goals covering protection and defense and creating the right workforce. It also includes a robust and growing identity management effort, including the issuance of more than 10 million common access cards (CAC) and a requirement from the Joint Task Force-Global Network Operations for CAC log-in with Public Key Infrastructure certificates.

There is yet another critical challenge – creating a Net-Enabled Command Capability (NECC). In addition to moving away from the current Global Command and Control System family of systems, this effort will also require a significant change in both mindset and approach. It will require moving from a static system and program-based acquisition environment to one that is dynamic and capabilities based. Also, it will change the current approach of *pushing* information to users, and instead will enable users to pull what they need and to contribute what they know. Instead of multiple architectures, it will be based on a single architecture. Perhaps most importantly, there will be a move from being platform specific and system driven, to platform independent and capable of dynamically meeting user needs.

As with many other aspects of the transformation, there are plenty of challenges for NECC in the months and years ahead. However, a program executive office has been established at DISA and an early 2006 Acquisition Decision Memorandum Exit Criteria was estab-

Coming Events

August 2-4
13th ISSAT (International Society of Science and Applied Technologies) International Conference on Reliability and Quality in Design
Seattle, WA
www.issatconferences.org/RQD2007page.htm

August 12-15
26th Annual ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing (PODC 2007)
Portland, OR
www.podc.org/podc2007

August 12-16
IWCMC (International Wireless Communications and Mobile Computing Conference) 2007
Honolulu, HI
http://dropzone.tamu.edu/~xizhang/IWCMC07/IWCMC07.htm

August 13-17
AGILE 2007 Conference
Washington, D.C.
www.agile2007.org

August 28-30
PerMIS '07
Performance Metrics for Intelligent Systems
Washington, D.C.
www.isd.mel.nist.gov/PerMIS_2007/index.htm

2008

Systems and Software Technology Conference
www.sstc-online.org

Coming Events: **Please submit coming events that are of interest to our readers at least 90 days before registration. E-mail announcements to: nicole.kentta@hill.af.mil.**

lished. Progress is indeed being made.

There are many other challenges that lie ahead. Most will require the innovative thinking that is best reflected by a sense of partnership with industry, academia, and technical associations. Success will be based on the ability to establish teams that are excited by the challenge, are ready to pursue new ideas, and can make things happen.

Summary

Information is a strategic asset. It is every bit as important as ships sailed, planes flown, and troops commanded, and, as an institution and a country, we must treat it as such.

Becoming net-centric is not about replacing the warfighter with technology. We will, for example, still need boots on the ground. Net-centric operations will allow humans to leverage information to better deal with unanticipated challenges, needs, partners, and circumstances.

Becoming net-centric means ensuring information is accessible throughout the enterprise from high-level headquarters and command centers to a soldier in a city tracking insurgents to a civilian at a depot in search of a new supplier. It centers on the knowledge that timely and trusted information can be shared with those who need it, whether alone or as a collaboration in groups.

Most importantly, becoming net-centric will allow the community to truly move to an information environment in which all participants, known and unanticipated, have confidence that they can get the information they need and they trust.

In the end, it comes down to a simple objective, one that is dear to our nation – saving lives. As we move into the future and deliver these capabilities to users across the enterprise, we must move as a team – a team that has a lot of challenging, yet very rewarding, work ahead. And I, for one, am looking forward to the journey.◆

References

1. DoD. The National Defense Strategy of the United States of America. Washington: DoD, 2005 <www.globalsecurity.org/military/library/policy/dod/nds-usa_mar2005.htm>.
2. DoD. The Quadrennial Defense Review Report. Washington: DoD, 2006.
3. DoD. The Net-Centric Data Strategy. Washington: DoD, 2003.
4. DoD. "Information Assurance Component of the GIG Integrated Architecture, Ver. 1.0." Washington: DoD, 2004.

About the Author

The Honorable John J. Grimes was nominated by President Bush on June 17, 2005 and sworn in as the Assistant Secretary of Defense for Networks and Information Integration/DoD CIO on November 14, 2005. He has extensive technical and policy experience in telecommunications, information systems, and the command and control fields. Grimes' public service includes the White House National Security Council Staff as Director for National Security Telecommunications Policy; Director of Defense Command, Control and Communications Programs; and Senior Director White House Situation Support Staff. He served as Deputy Assistant Secretary of Defense for Defense-wide Command, Control, and Communications and was the Deputy Assistant Secretary of Defense for Counterintelligence and Security Countermeasures. As a member of the DoD senior executive service, Grimes held senior technical and staff positions with the National Communications System; Defense Communications Agency; and the U.S. Army Communications Command following his military service in the U.S. Air Force. Previously with Raytheon, he served as Vice President of Intelligence and Information Systems, Washington Operations. Grimes has served on four Defense Science Board Task Forces and was a member of the Industry Executive Subcommittee of the President's National Security Telecommunications Advisory Committee. Grimes is a graduate of the University of Arizona, and has a master's degree from Shippensburg University in Pennsylvania. He is a graduate of the U.S. Army War College, Carlisle Barracks, Pennsylvania; the Federal Executive Institute, Charlottesville, Virginia; and Harvard University's National and International Security Policy program. He is the recipient of the American Institute of Aeronautics and Astronautics' Command, Control, Communications, and Intelligence award among other public, military and federal civil service awards, including two Presidential Rank awards.

6000 Defense Pentagon
Washington, D.C. 20301-6000

Sharing Information Today: Net-Centric Operations in Stability, Reconstruction, and Disaster Response

Dr. Linton Wells II
Principal Deputy Assistant Secretary of Defense (Networks and Information Integration)

As the Department of Defense (DoD) continues its information age transformation to net-centric operations, we must consider the full array of the DoD's activities. The level of interaction with partners outside the boundaries of DoD networks has increased tremendously over the past few years. In particular, it is crucial to support Stability, Security, Transition and Reconstruction (SSTR) operations, Humanitarian Assistance and Disaster Relief (HADR), and Building Partnership Capacity (BPC) among potential coalition members. The social, political, and economic goals for which United States and coalition forces are committed can only be achieved through effective interaction with these non-traditional partners in largely unclassified environments.

Net-centric operations are key elements of the DoD's information age transformation. Much has been written about net-centric approaches in major combat operations. However, the DoD also must be able to support SSTR operations, HADR, and BPC among potential coalition members. Net-centric principles must extend to these environments as well.

Thus, it is necessary to communicate, collaborate, engage, and – in some cases – translate with civil-military partners outside the boundaries of DoD networks in what often are called *complex operations*. These capabilities are not nice-to-have adjuncts to other military requirements. In fact, the social, political, and economical goals for which United States and coalition forces are committed *cannot* be achieved without the ability to interact effectively with these non-traditional partners in largely unclassified environments. Such collaborative efforts need to work with austere communications that function where power is unreliable. These capabilities are urgently needed now in Iraq and Afghanistan, and they will be needed elsewhere in the future.

As has often been said, there is no interoperability without operability. Real-world experiences – from the Balkans to Iraq and from the tsunami relief to Katrina – have shown that operations repeatedly have been impeded by a lack of *communications, lift,* and *power*.

Communications

Networks provide a means to share information, develop shared situational awareness, and self-synchronize actions in accordance with command intent to accomplish its mission more effectively. But the sensors to gather data, and the ability to share information, are not techie-geek adjuncts to major muscle movements such as the delivery of food, water, and shelter. *They are critical enablers of everything else that happens.* Such capabilities often are called *hastily formed networks* and they are essential to restoring basic voice and data services, both in disaster and stability environments. The network environment during the initial phases of a disaster response often is chaotic. Organizations may arrive with their own networks and promptly activate systems without coordinating with other participants. Radio frequency management is seldom done well. As a result, Information and Communications Technology (ICT) leaders in disaster areas must coordinate actions prior to activating their networks to minimize these types of problems. More generally, technical solutions must provide the flexibility to add unanticipated users, connect with non-traditional partners, scale to meet demands for bandwidth, and support the users with intermittent connectivity who always are involved in emergencies.

> *"Trust is essential for relationships to be established, on or offline, and for actions to be taken in stressed environments."*

Lift

Networks and their supporting equipment almost always will have to be moved into crisis locations, either to augment damaged systems or add new capabilities. But, too often, they are not given adequate priority in lift manifests to get there soon enough to enable the other actions that depend on them. Such capabilities need to be put on the first few lifts during an operation and not be relegated to follow-on echelons.

Power

Stable, reliable electrical power is essential for effective information sharing, but almost never was available in HADR environments and rarely in SSTR. In such situations, power solutions ideally would not depend on gasoline or diesel fuel, which complicate the already significant logistic problems in austere environments. Several efforts are beginning to produce rapidly deployable, sustainable power systems that can use multiple energy sources (wind, solar, biofuel, etc.), and these should be incorporated into exercises and contingency plans.

Social Networking

Technology is an important component of information sharing, but by no means the only one. Social networking is a key enabling function in fostering effective responses to complex emergencies. Trust is essential for relationships to be established, on or offline, and for actions to be taken in stressed environments. Such trust is not built overnight. It needs to be built on shared experiences and reinforced with credible identification management. The establishment of relationships with anticipated partners, well before a contingency, is critical to the success of future operations.

Data Strategy

A core tenet of net-centric operations is the underlying data strategy. This calls for data to be visible, accessible, and understandable, even for unanticipated users. The approach decouples data and applications, enabling much more flexible responses, but it also requires that data from diverse sources be tagged appropri-

ately. This can be a particular challenge when dealing with a wide range of partners. Moreover, merely creating information is not enough. This goal is to support improved decision-making and to turn decisions into actions as quickly as possible. This often involves innovation in the field.

Entrepreneurial Adaptation

The pace of technological change is breathtaking, and government systems, however well resourced, typically developmentally lag in the private sector. Moreover, planned linkages and interactions will almost certainly be overtaken by events in crises. Therefore, a critical component of an effective response is to be able to adapt existing capabilities in cooperative, entrepreneurial ways on the fly.

By taking these lessons into account, the DoD is working on five parallel fronts to extend net-centric operations to SSTR, HADR, and BPC environments:

1. Developing *capabilities* to gather situational awareness and to share it by communicating, collaborating, translating, and engaging beyond the boundaries of the *.mil* domain with non-traditional, civil-military partners in a wide variety of situations.
2. Cultivating diverse *social networks* and having them ready both to deploy quickly and to be received as trusted partners by anticipated and unanticipated partners on the scene. The DoD and its civil-military partners need to be able to assemble and share lists of available practitioners and their skill sets in trusted electronic environments.
3. Incorporating best practices *to change concepts of operations; doctrine; and tactics, techniques, and procedures*, so that appropriate action can be taken by forces on the scene without having to constantly refer issues back to higher authority.
4. Implementing *modest legal changes* that allow ICT to be used more broadly in reconstruction and repair and allow for capabilities to be left behind after the end of an operation.
5. Providing *some funding* (not much, but quickly available) to deploy these capabilities with trained personnel early enough to let them act as the critical enablers of other activities.

These approaches can transform our information sharing capabilities and greatly improve the DoD's capabilities in the critical areas of SSTR, HADR, and BPC. Establishing resilient networks and power grids in affected areas must be planned for and executed early to enable information sharing, enhance the resiliency of the local populace, and accelerate an effective response.◆

About the Author

Linton Wells II, Ph.D., serves as the Principal Deputy Assistant Secretary of Defense (ASD) (Networks and Information Integration [NII]) and was recently selected to serve as the Chair of Force Transformation and Distinguished Research Professor at the National Defense University. Prior to this, he served in the Office of the Under Secretary of Defense. Wells has more than 26 years in the U.S. Navy and has served in a variety of surface ships, including command of a destroyer squadron and guided missile destroyer. He has a bachelor's degree in physics and oceanography from the U.S. Naval Academy and a master's degree in engineering and a doctorate in international relations from The Johns Hopkins University. Wells is also a graduate of the Japanese National Institute for Defense Studies in Tokyo and was the first U.S. naval officer to attend.

SES
Principal Deputy ASD/NII
6000 Defense Pentagon
Washington, D.C. 20301
Phone: (703) 614-7323
E-mail: linton.wells@osd.mil

Web Sites

The United States Department of Defense Chief Information Officer

www.defenselink.mil/cio-nii/

The Department of Defense Chief Information Officer (DoD CIO) Web site is the homepage of the DoD CIO, offering links to legislation, policy, and communities of interest resources, as well as links to publications and articles produced by the DoD CIO. The DoD Information Strategic Plan can be found at <www.dod.mil/cio-nii/docs/DoD_IA_Strategic_Plan.pdf>. The DoD is implementing an ongoing strategic management process to enable the information assurance (IA) community to implement and manage strategic decisions, respond dynamically to changing conditions, and evolve the strategy as the situation dictates. Their ability to successfully achieve the goals in this plan requires the continued commitment and mandate from senior leadership and the cooperative support of all members of the IA community. The IA strategic plan is a living document that will continue to be reviewed for the DoD's vision, goals and objectives for relevancy, currency, and applicability to keep pace with the changing environment and address significant challenges they face.

Defense Information Systems Agency

www.disa.mil

The Defense Information Systems Agency is a combat support agency responsible for planning, engineering, acquiring, fielding, and supporting global net-centric solutions to serve the needs of the President, Vice President, the Secretary of Defense, and other DoD components, under all conditions of peace and war. They are the provider of global net-centric solutions for the nation's warfighters and all those who support them in the defense of the nation.

The Association for Enterprise Integration

www.afei.org

The Association for Enterprise Integration (AFEI) is the leading industry group providing a framework for collaboration between government and industry. The DoD CIO has turned to AFEI to be its conduit for policy and strategy input from industry through jointly chartered working groups. Scheduled events, the resource library, and news can all be accessed without membership on the Web site.

Getting to GIG: Enterprise-Wide Systems Engineering

Defense Information Systems Agency

The Defense Information Systems Agency (DISA) has recently taken on a new initiative to perform Enterprise-Wide Systems Engineering (EWSE), expanding upon the work currently performed by the Assistant Secretary of Defense for Networks, Information, and Integration (ASD[NII]) staff. DISA is leveraging their vast technical resources to perform end-to-end systems engineering across the Global Information Grid (GIG) to jump start this effort.

The goals of EWSE include providing continuous oversight of the GIG's evolution, maintaining a GIG enterprise-wide technical baseline, establishing enterprise-wide analysis capabilities, establishing a GIG compliance management program, and overseeing enterprise-wide experiments.

DISA's GIG engineering directorate is leading this effort and recently stood up the new EWSE Management Office to coordinate activities across DISA sub-units and to provide interfaces to ASD (NII) and other organizations outside DISA, including the National Security Agency (NSA), Naval Research Laboratory, Coordinating Committee for Multilateral Export Controls, Services, and other Department of Defense (DoD) agencies. The EWSE office will also prioritize workload and develop annual work plans. A major focus of the effort will be to resolve GIG EWSE issues for end-to-end interoperability including incrementally developing a common set of requirements for capabilities that span the GIG, establishing a GIG end-to-end reference architecture, developing technical guidance to facilitate end-to-end interoperability and performance, and developing a minimum set of interoperability and performance requirements (i.e. Net-Centric Interface Documents [NCIDs]) for GIG programs and systems.

Specific technical issues to be resolved by the new EWSE team include:

Black Internet Protocol (IP) Core Architecture. The EWSE team will develop a flexible and affordable black IP core architecture that provides external encryption to the tactical edge of the GIG. This architecture extends the black core to bases, posts, camps, and stations and to service delivery points for tactical (mobile, deployable, transportable) networks and will provide critical insight in supporting the fiscal year (FY) 2010 program office memorandum build. This effort will define a solution for GIG gateways, service delivery points and defense integration systems network interfaces.

Voice-over IP (VoIP). The EWSE team will define a GIG end-to-end VoIP architecture. It will develop associated VoIP requirements, standards, interface specifications, and performance criteria for all DoD enterprise component systems. This initiative will provide a standards-based documented architecture and guidance that will enable multi-vendor implementations.

Operationalizing GIG Quality of Service (QoS). The EWSE team's objective is to demonstrate the feasibility of a proposed QoS approach. It will define a QoS service class definition for DoD needs and define service level objectives and performance metrics for QoS service classes. It will leverage modeling and simulation efforts to validate QoS performance requirements and architecture decisions.

GIG Services. The EWSE team will develop an interoperable architecture for GIG services and address core enterprise services issues for study as a result of Program Decision Memorandum III (PDM III). The EWSE team will provide a liaison and coordinate with the various core enterprise services working groups chartered under PDM III. They will identify key issues to be addressed, document results of the studies in NCIDs, and ensure that proposed solutions trace to and are consistent with the rest of the GIG technical guidance.

Information Assurance (IA). Working with NSA, this effort builds on the current GIG IA Architecture. This work will expand in FY 2007 to focus on IA enterprise system engineering and the development of an IA implementation plan and guidance. The task will also develop an acceptable High Assurance IP Encryptor discovery solution and develop implementation guidance for cross-domain solutions to manage and control information.

Tactical Edge Issues. The EWSE team's goal is to address tactical edge issues articulated by the joint net-centric operations portfolio manager focusing on tactical ground and tactical ground-to-air scenarios. This effort will involve developing solutions for issues such as address allocation, mobile domain routing, tactical QoS for voice and data, and tactical network management.

The EWSE effort also involves maintaining and ensuring compliance with the GIG Technical Baseline by working with programs to define requirements. This close working relationship with program offices throughout the DoD was established through DISA's role as the DoD Executive Agent for Information Technology (IT) Standards. Within this context, the Enterprise Documentation Framework working group was set up to streamline technical baseline documentation and perform configuration management. The DoD IT Standards Registry (DISR) is evolving to fit the new tech baseline. Program office technical staffs will be able to access the latest standards and GIG technical guidance published to the DISR with just a few mouse clicks.

Applying an EWSE approach to next-generation GIG capabilities will improve DoD acquisition decisions based on solid technical advice. The effort will instantiate department-wide, detailed, technical analysis by defining fundamental GIG interoperability and performance requirements for both warfighting and business capabilities. The analysis is targeted at addressing risk and synchronization across programs, and the improved decision process will enable the deployment of new or improved capabilities quicker or at lower cost. GIG EWSE is critical to ensure acquisition and interoperation of GIG components that will result in end-to-end capabilities enabling warfighters to better conduct agile net-centric operations.◆

About DISA

This article was the collaborative effort of several individuals from DISA. DISA is a DoD combat support agency under the direction of ASD (NII). It is responsible for planning, engineering, acquiring, fielding and supporting global net-centric solutions and operating the Defense Information System Network to serve the needs of the President, Vice President, Secretary of Defense, Joint Chiefs of Staff, Combatant Commanders, and other DoD components under all conditions of peace and war. More information on DISA and the GIG can be found at <www.disa.mil/index.html>.

Providing the Tools for Information Sharing: Net-Centric Enterprise Services

Ann H. Kim and Carol Macha
Department of Defense Chief Information Officer Information Policy Directorate

The Department of Defense (DoD) is establishing a net-centric environment that increasingly leverages shared services and Service Oriented Architecture (SOA) that, among other things, is supported by the required use of a common and shared infrastructure. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. The Net-Centric Enterprise Services (NCES) program is a transformational program that delivers a set of shared services as part of the DoD's common infrastructure to enable networked joint force capabilities, improved interoperability, and increased information sharing across mission area services.

As the DoD continues to face new and evolving threats, it must be poised to quickly respond to those threats with an increased level of agility. The DoD recognizes that this level of agility requires a fundamental change in the way information technology is provided and managed by the DoD. With the publication of the Net-Centric Services Strategy [1] the DoD has established a vision for achieving this agility through the use of shared services and SOAs.

The DoD Net-Centric Services Strategy outlines an approach in which the DoD's wide range of information and functional capabilities – provided by our many systems – are made available through software-based services on enterprise networks. These software-based services deliver reusable business functionality as standardized *building blocks* that can be quickly adapted into capabilities that meet rapidly changing mission needs.

To achieve this vision of a services-based environment, the DoD must establish a common infrastructure that will enable networked joint force capabilities, improved interoperability, and increased information sharing across mission area services. The objective of the NCES program is to deliver a set of shared services as part of this common infrastructure.

The NCES is a Defense Information Services Agency acquisition program to adopt, buy, or create essential information sharing services needed by the DoD. As part of the common infrastructure, it will enable seamless information sharing by providing enterprise-wide services for characterizing, cataloging, locating, and accessing information on the Global Information Grid (GIG). NCES is the only program specifically tasked with providing enterprise-wide information sharing capabilities to enable information superiority, accelerated decision-making, and effective operations.

This groundbreaking program faces the following significant challenges:

Establishing Trust. As a provider of shared enterprise services, NCES has a vested interest in facilitating the cultural shift within the DoD to establish trust in the availability of services provided outside of one's own organization. A secure, agile, and interoperable services-based environment in which information is much more readily visible and accessible to the DoD, as well as other authorized federal, state, local, and coalition partners requires the establishment of trust on multiple levels. The success of NCES depends on the establishment of mechanisms to enable trust in the capabilities (availability), trust in the information (assurance), and trust in the participants (identity).

NCES' services must be made available across the DoD. Its user community spans strategic, operational, and tactical networks. To facilitate trust in NCES' services, the NCES program must be able to define service level agreements (SLAs) that describe the reliability and performance of its services for its many users across the different networks. It needs to publish those SLAs and instrument its services such that they can be monitored against the SLAs. As a result of two recent DoD Chief Information Officer (CIO) reports [2, 3], the NCES program is actively working with the Joint Task Force-Global Network Operations (JTF-GNO) to identify needed capabilities for operating and monitoring information sharing capabilities offered as services on the GIG.

To establish trust in NCES as a service provider, the program has established the Early Capabilities Baseline through which users and organizations have an early opportunity to use NCES' services and provide feedback to the program. This early interaction allows NCES to develop relationships with its user community, to demonstrate utility across their environments, and to continuously involve its stakeholders in the refinement of its enterprise services.

Scaling to the DoD Enterprise. NCES' services are currently being developed to support an estimated number of users. However, as the DoD's implementation of services and SOAs mature, the value of information reuse and readily found capabilities will be recognized. The program must plan for its services being leveraged in the development of information sharing capabilities by unanticipated but authorized users across the DoD and its mission partners. Any initial load balancing and scalability thresholds could very quickly be exceeded.

Through NCES' collaboration with the JTF-GNO to identify capabilities for operating and monitoring shared enterprise services, the program is proactively developing long-term solutions to this challenge. The technical solution must be augmented by an appropriate resourcing model that enables the program to continue providing services according to published SLAs and accommodate growth in demand.

Governance. Widespread adoption of NCES' services into business/mission processes requires the establishment of governance around their provisioning, security, use, and operation. NCES' services must be based on common standards and rules to ensure interoperability and consistent implementation throughout the DoD. The DoD must establish a governance framework that ensures that the common standards and rules are consistently applied and enforced.

The NCES program, in collaboration with the DoD community, has been developing an enterprise services governance framework that addresses this challenge. This framework should provide limited, lightweight enterprise governance for

Continued on Page 16

Making It Work – The Net-Centric Global Information Grid NetOps Strategy

Thomas Lam
Office of the Assistant Secretary of Defense

The Joint Network of Operations (NetOps) Concept of Operations is assigning overall responsibility for NetOps to Commander, United States Strategic Command (CDRUSSTRATCOM) and has enabled the Department of Defense (DoD) to begin improving the operations and defense of the Global Information Grid (GIG). However, there is still only limited progress in implementing an enterprise-wide construct that fully addresses all aspects of NetOps in a dynamically changing global environment. Observations from Operation Iraqi Freedom (OIF) continue to reinforce that the DoD has only limited abilities to provide commanders with relevant and timely GIG situational awareness or mission impact assessments and that lack of abilities to effectively de-conflict, coordinate, and control spectrum use represents a very real and operationally critical problem that must be solved. These deficiencies coupled with sometimes confusing or even conflicting policies and guidance, significantly impact the ability of the operators/defenders of the GIG to fully support ongoing warfighting and peacekeeping missions in an increasingly joint and multi-partner environment. To provide a way ahead and to foster unity of effort across the DoD, the DoD Chief Information Officer (CIO) is developing the Net-Centric GIG NetOps Strategy to describe a net-centric vision and mission for GIG NetOps along with the necessary high-level goals and objectives.

The Joint NetOps Concept of Operations and assignment of overall responsibility for NetOps to CDRUSSTRATCOM has enabled the DoD to begin improving the operations and defense of the GIG. However, there is still limited progress in implementing an enterprise-wide construct that fully addresses all aspects of NetOps in a dynamically changing global environment. Observations from OIF continue to reinforce the following:

- There is only limited ability to provide commanders with relevant and timely GIG situational awareness or mission impact assessments.
- There are confusing and sometimes conflicting NetOps policies and guidance.
- There is limited ability to de-conflict, coordinate, and control spectrum use.

Across the DoD, there is little, if any, coordination or synchronization amongst the many independent NetOps acquisition and fielding activities that are currently under way. Additionally, there is a general lack of metrics and processes to measure the health and readiness of the GIG. These deficiencies significantly impact the ability of the operators/defenders of the GIG to fully support ongoing warfighting and peacekeeping missions in an increasingly joint and multi-partner environment.

To provide a way ahead and to foster unity of effort across the department, the DoD CIO is developing the Net-Centric GIG NetOps strategy to describe a net-centric vision and mission for GIG NetOps along with the necessary high-level goals and objectives. Highlights of the strategy are introduced in this article.

Vision and Mission of Net-Centric GIG NetOps

The vision for Net-Centric GIG NetOps is to transform existing and new capabilities into a force multiplier that enables the warfighting, business, intelligence and enterprise information environment mission areas to fully employ the power of the GIG. The corresponding mission is to enable the DoD to employ the GIG as a unified, agile, and adaptive enterprise that does the following:

1. Facilitates Net-Centric Operations (NCO) by enabling authorized users and mission partners to access and share timely and trusted information from any location at any time.
2. Ensures that GIG capabilities can be fully employed as a joint weapon system that meets warfighter mission needs and priorities.

"The vision of the Net-Centric GIG NetOps is to transform existing and new capabilities into a force multiplier that enables the warfighting, business, intelligence and enterprise information environment mission areas to fully employ the power of the GIG."

As shown in Figure 1 (see page 12), NetOps forms the core of GIG operations in a net-centric framework and is a critical enabler of the NCO. NetOps (center) ensures that the key components of the GIG (transport and computing infrastructure, data, services, and information assurance) create a supportive environment (inner ring) that protects and maintains the integrity and quality of information (middle ring), thereby ensuring that users can easily post, access, and share relevant information and collaborate to conduct NCO (outer ring).

Goals of Net-Centric GIG NetOps

The Net-Centric GIG NetOps goals are focused on achieving positive operational mission outcomes and reflect an emerging recognition across the department that the majority of the challenges associated with transforming NetOps into a net-centric enabler are organizational or cultural in nature.

Goal 1: Enable authorized users, including mission partners, to access and share information and collaborate at any time, from any location.

Fundamental to the mission of Net-Centric GIG NetOps is to enable authorized users (including mission partners)

to access and share information and collaborate among those involved from any location at any time within the limitations imposed by technology, deployed GIG capabilities, laws, and policies. Achieving this goal will require that NetOps play a dual role with respect to the Net-Centric Data Strategy. NetOps must be able to manage and facilitate the visibility, accessibility, and understandability of information, along with the ability to share information within and across DoD mission areas. NetOps data must also be made visible, accessible, and understandable to all authorized users to facilitate end-to-end GIG situational awareness.

Goal 2: Enable the DoD to employ the GIG as a unified, agile, and adaptive joint weapons system that meets warfighter mission needs.

The DoD's growing dependence on the GIG as the primary means of enabling and delivering a wide variety of command and control to decision makers at all levels highlights the need for reconsidering how this critical warfighting capability is perceived, employed, and managed. Ensuring that the combatant commands can effectively employ the GIG will require that it be dynamically operated and employed as a single unified agile and adaptive enterprise, responsive to the holistic needs of the DoD priorities and goals. Having the ability to maneuver critical data or employ GIG capabilities when and where they are needed most or to rapidly change the configuration of the GIG in response to changing mission parameters will significantly enhance the value of the GIG to the warfighter and allow the warfighter to fully and confidently leverage the power of GIG.

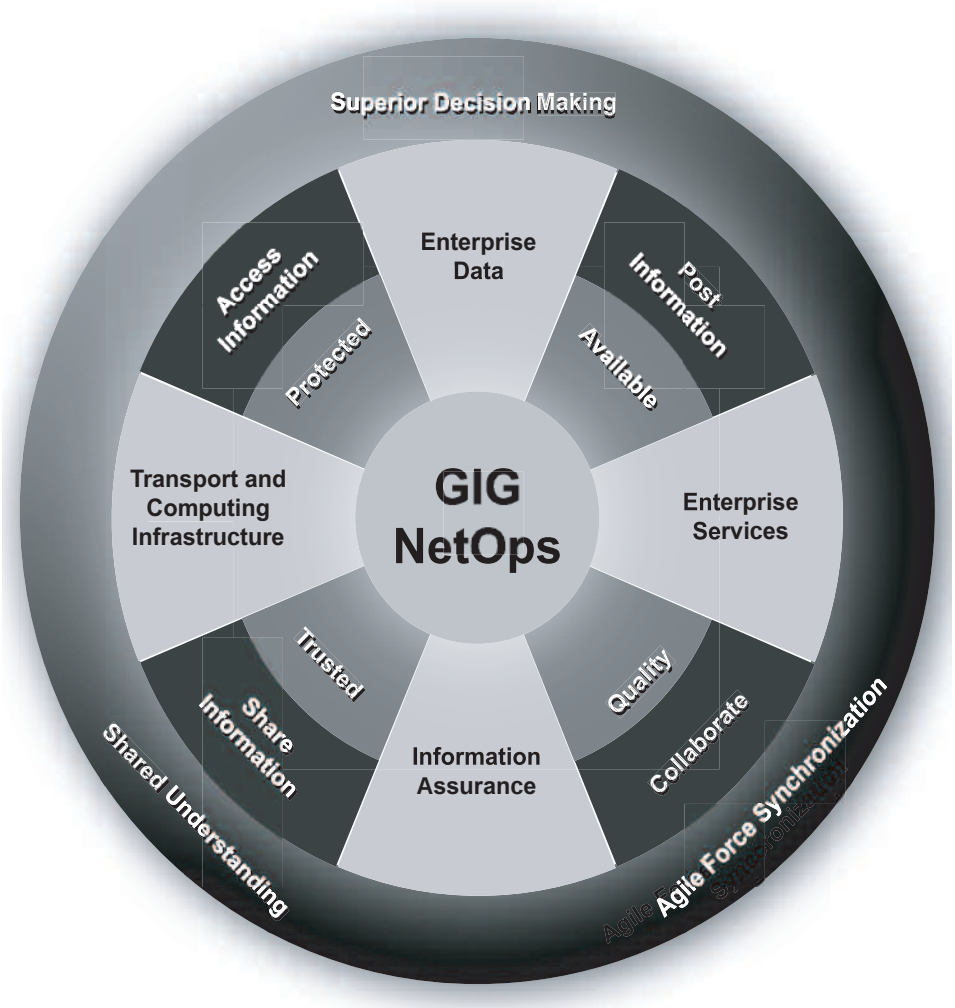
Goal 3: Co-evolve and mature NetOps *in-stride* with GIG capability increments.

As GIG capabilities are transformed to support NCO, it will be critical to implement and mature NetOps capabilities in a structured and consistent fashion. It will require that NetOps capabilities be developed and deployed as time-phased capability increments that are consistent with the defined GIG capability increments and support them. A critical aspect of NetOps transformation is the creation of policy, governance structure, implementation plans, and metrics for measuring progress that will be necessary to guide NetOps evolution.

Conclusion

Developing, designing, deploying and operating future GIG NetOps capabilities and forces will require a unity of effort across the DoD. It will require active participation from across the broadest possible cross-section so that the DoD can achieve the common goal of a GIG that can be effectively employed to support the many missions of the DoD in an increasingly joint and multi-partner environment.◆

Figure 1: *Core of Net-Centric Framework*



About the Author

Thomas Lam is the Office of the Assistant Secretary of Defense (NII) DoD CIO NetOps Lead. He led the development of the DoD Net-Centric GIG NetOps Strategy. He assists the DoD CIO as the principal staff assistant and advisor to the Secretary of Defense and Deputy Secretary of Defense on NetOps in directing and overseeing various NetOps activities across the DoD. Lam has more than 25 years of experience in the design, development, and implementation of telecommunication systems and NetOps solutions. During the last 20 years with the Defense Information Systems Agency, he held various engineering and management positions. Lam has a bachelor's degree in electrical engineering from George Washington University, a master's degree in electrical engineering from Rensselaer Polytechnic Institute, and completed the Office of Personnel Management Executive Leadership Development program.

OASD (NII) DoD CIO
Architecture and Interoperability Directorate
1851 S Bell ST STE 7000
Arlington, VA 22202
Phone: (703) 607-0597
Fax: (703) 607-0248
E-mail: thomas.lam@osd.mil

Securing the Global Information Grid – The Way Ahead for Information Assurance

Richard Aldrich
Booz Allen Hamilton

David Zaharchek
IBM

The Department of Defense's (DoD) Information Assurance (IA) Strategic Plan provides a solid foundation and framework for securing the information, and the DoD has realized several significant accomplishments across each of five goals to effectively increase the DoD's security posture of the DoD. Our future success will require a continued focus on the operational aspects of IA to combat current and future threats in real-world operational environments. The threats facing the DoD are real. Our networks are under attack daily and our adversaries are growing ever more sophisticated. To effectively defend its systems and networks, the DoD is implementing a multi-layered, defense-in-depth approach.

A 2006 report released by the General Accountability Office (GAO), titled *Suggested Areas for Oversight for the 110th Congress* [1], provided recommendations for 36 oversight areas for the incoming 110th Congress. One recommendation included in the GAO report suggested the DoD develop and implement viable strategic plans with goals, objectives, key milestones, and measures to monitor and report on progress in transforming its key business operations. The DoD IA community has outpaced the GAO's recommendation by several years and has set the standard for strategic planning within the DoD. The DoD IA Strategic Plan, released in January 2004, provides a solid foundation and framework for securing the DoD's information, defines the DoD's goals and objectives for IA, and provides a consistent, department-wide approach for securing the Global Information Grid (GIG). The DoD IA Strategic Plan has been instrumental in defining the value proposition and building a convincing business case for IA – resulting in more than 54 percent real growth in the DoD's IA budget since 1999.

The cornerstones of the IA Strategic Plan are its five goals:

- **Goal 1: Protect information.** Safeguarding data to ensure that the level of trust for all information corresponds with mission needs.
- **Goal 2: Defend systems and networks.** Recognizing, reacting to, and responding to threats, vulnerabilities, and deficiencies.
- **Goal 3: Provide integrated IA/ Network Operations (NetOps).** Providing decision-makers and network operators at all command levels with the tools to conduct IA/ Computer Network Defense (CND) operations and net-centric warfare.
- **Goal 4: Transform and enable IA capabilities.** Discovering emerging technologies, experimenting, improving process life-cycle time, reducing risk exposure, and increasing return on investment.
- **Goal 5: Create an IA empowered workforce.** Establishing an IA professional workforce with the right skills, in the right place, at the right time.

These goals are enduring and serve to define a consistent strategic direction to keep information secure and trusted while at the same time accessible. The DoD has realized several significant accomplishments across each of the five goals to effectively increase the security posture of the DoD; however, while the DoD has made tremendous progress in defining requirements, developing policies and processes, and developing and deploying innovative technical solutions to the warfighters, our future success will require a continued focus on the operational aspects of IA – fusing people, processes, and technologies – to combat current and future threats in real-world operational environments.

Efforts are under way to ensure personnel have the knowledge and skills to effectively and securely operate and defend the DoD's information systems and networks. The DoD IA Scholarship Program is a highly competitive initiative that provides full scholarships to students who attend National Security Agency-designated centers of academic excellence in IA education in exchange for DoD service. Scholarships are used to recruit new personnel into the DoD and to provide opportunities for current employees to earn advanced degrees in IA related disciplines.

A second, and much broader, initiative is the IA Workforce Improvement Program. Its focus is managing and professionalizing the IA workforce. To do this, the program leverages commercial information technology security certifications, such as those offered by International Information Systems Security Certification Consortium, Information Systems Audit and Control Association, System Administrator, Audit, Network, Security Consortium, Computing Technology Industry Association, and Security Certified Program, to establish a DoD baseline of IA workforce knowledge and skills. All personnel performing IA functions – military, civilian, and contractor – are expected to meet the requirement, whether they do the work as a primary duty or as an additional or embedded duty. Currently, components are in the process of identifying and documenting their IA workforce and preparing them to be certified to the DoD-wide baseline.

The DoD is a robust, worldwide organization that leverages its capabilities through information systems and networks. The increasing reliance upon these information systems and networks for our nation's defense makes their protection critically important. As the DoD becomes more net-centric, it becomes more vulnerable to shared risks where the vulnerabilities of one part of the network could adversely impact many others.

The threats facing the DoD are real. Our networks are under attack daily and our adversaries are growing ever more sophisticated. The DoD's information infrastructure, the GIG, globally pervasive and comprised of millions of hosts and thousands of networks, is subject to hundreds of thousands of attacks, scans, and other incidents every year. To effectively defend its systems and networks, the DoD is implementing a multi-layered, defense-in-depth approach. Some of these enterprise defense-in-depth initiatives include the following:

- The fielding of two commercial tool suites, one to scan for vulnerabilities (Secure Configuration Compliance Validation Initiative) and one to remediate them (Secure Configuration Remediation Initiative). The tools can also

check for compliance with best security practices as specified in the DoD's security technical implementation guides and take remedial actions as appropriate. Using these tools, the system administrators can rapidly identify and patch vulnerabilities.

- Increased protection measures on each computer and server. The DoD will soon deploy an enterprise-wide host-based security system capability that will field an integrated package of host-based security applications to help fight today's dynamic network threats. These include the intrusion detection system, host-based intrusion prevention system, host-based firewall, file integrity monitoring and alerting, execution control, self-enforcing configuration control, and information condition management capability. As the DoD increasingly encrypts its communications to the end user, bolstering defenses at the host level is becoming critical.
- Two initiatives supporting insider threat mitigation. One effort is directed broadly at detecting the threat and the second is focused on monitoring those who are suspected insiders. Contracts for this enterprise capability should be awarded in the near term.
- Attribution capability to identify the originators of cyber attacks. This capability is key to the appropriate NetOps response. As such, the DoD has initiated a bolstered forensics effort that will facilitate detailed analysis of systems that were attacked. In addition, the DoD is also developing a *honeygrid* capability as a means of identifying, distracting, and diverting attackers.
- Hardening of the DoD's IT infrastructure with additional firewalls and demilitarized zones (DMZs). The DMZ approach provides a separate interface to the Internet and external DoD connections, thus limiting nonclassified Internet Protocol Router Network vulnerabilities to malicious attacks, worms, and viruses that plague the Internet. The DMZ also mediates and regulates external access to DoD applications, data, and public information services pages.

Deployment and distribution of enterprise security tools have been accomplished by various means. These include direct download of the software licenses from the DoD server to the individual user/system administrator as well as direct installation of tools by the DoD or integration contract resources to implement the tools within a local site. Tools designated for general use throughout the enterprise are normally operated by the system administrators at each of the component enclaves. However, a centralized help desk, supporting most of the enterprise capabilities, has been established within the Defense Information Systems Agency to provide information and assistance for tool installation and operation for all DoD users.

Components receive updates to enterprise tools as well as new capabilities through either the normal component budgeting process and/or in combination with the DoD enterprise solutions steering group. This steering group provisions general CND tools enterprise-wide based on identified requirements and funding constraints.

The DoD recognizes securing this vast network of networks requires more than technological solutions. To synchronize these efforts, the DoD developed an IA component of the GIG architecture that defines required capabilities to secure the GIG. These have been further defined as the IA capability areas and are managed as an IA capability portfolio. Portfolio management has been fully embraced by the DoD and provides a framework for analyzing IA investments. The GIG IA Portfolio Management Office manages the IA Capability Portfolio by looking at the many initiatives being funded by elements across the DoD in a disciplined and unified manner, aligning these investments against the GIG IA architecture and the IA Strategic Plan and projecting anticipatory research to address critical challenges in securing the GIG.

The threat environment is constantly changing and evolving, unconstrained by state and national borders. To overcome these challenges, the DoD is diligently working to improve and harden its defenses while expanding cooperation with national and international partners. The IA strategic plan lays the foundation for securing the GIG. However, our future success requires the dedication, commitment, and personal vigilance on the part of all GIG users. In addition to our efforts to secure the GIG through the deployment of new capabilities and the establishment of policies, we must establish a climate of security consciousness, commit resources, organize and train personnel, and accept responsibility for protecting the GIG to achieve mission success. Securing the GIG is the responsibility of us all.◆

Reference

1. "Suggested Areas for Oversight for the 110th Congress." Washington: GAO, 2006 <www.gao.gov/new.items/d07325r.pdf>.

About the Authors

Richard Aldrich is the senior computer network operations policy analyst for the Information Assurance Technology Analysis Center and an associate for Booz Allen Hamilton. He has multiple publications in information security and has presented at several national and international conferences. He has a bachelor's degree in computer science from the U.S. Air Force Academy, a Juris Doctor from the University of California Los Angeles, and a Master of Laws in Intellectual Property Law from the University of Houston.

Booz Allen Hamilton
1215 S Clark ST
STE 1101
Arlington, VA 22202-4302
Phone: (703) 602-9991
Fax: (703) 602-7209
E-mail: richard.aldrich.ctr@osd.mil

David Zaharchek is a managing consultant in IBM Business Consulting Services' Public Sector Business Strategy Practice and has supported strategic planning and performance measurement efforts for the DoD Defense-Wide Information Assurance Program for more than five years. Zaharchek has both public and private sector experience in the areas of corporate strategic planning, strategic resource allocation, and performance measurement and management.

IBM Business Consulting Services
1215 S Clark ST
STE 1101
Arlington, VA 22202-4302
Phone: (703) 653-7028
Fax: (703) 602-7209
E-mail: david.zaharchek@us.ibm.com

Spiraling Information Demands – The Way Ahead With IPv6

Kristopher L. Strance
Office of Assistant Secretary of Defense

The achievement of Net-Centric Operations and Warfare (NCOW), envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms, facilities, people, and information, depends on effective implementation of Internet Protocol Version 6 (IPv6) in concert with other aspects of the GIG architecture.

– Department of Defense Chief Information Officer (DoD CIO) Memorandum, June 2003

IPv6 is the next-generation network layer protocol for the Internet and the DoD GIG.

The current version of IP, IPv4, was developed in the 1970s and is the basis of interoperability for today's Internet and many DoD networks. However, IPv4 has limitations that inhibit the end-to-end paradigm of the Internet and achievement of the DoD's vision of net-centric operations.

IPv6 has been under development by the Internet community for more than a decade and is designed to overcome IPv4 limitations by greatly expanding available IP address space and integrating features such as end-to-end security, mobile communications, Quality of Service (QoS), and simplified network management. The numerous fixes and extensions implemented to overcome IPv4 limitations often have increased network complexity and slowed network performance. The DoD transition to IPv6 will add functionality and reduce network complexity.

Why Is IPv6 Transition Important to the DoD?

The DoD seeks to build a *more* agile, robust, interoperable, and collaborative net-centric environment where warfighters, intelligence, and business users share information on a secure, dependable, and global network. This NCOW network will enable superior decision-making and more effective military operations through network ubiquity and scalability, globally routable addresses, network support of QoS, enhanced plug-and-play/mobility, auto-configuration, improved multicast, end-to-end security, and improved network maintainability.

In the GIG, IP is the common network protocol that allows all types of data to move seamlessly on the GIG's diverse transport layer which includes landline, radio, and space-based elements. Due to fundamental limitations of the current IPv4 protocol for the long-term networking requirements of the DoD and commercial community, IPv6 is a critical enabler in achieving the DoD's vision of the NCOW.

Challenges of Transitioning to IPv6

The DoD strategy for transitioning to IPv6 is based on technology refreshment of the DoD Information Technology (IT) infrastructure. This poses a daunting challenge since this infrastructure is distributed across all DoD components, geographically dispersed, and managed through a complex and interdependent mesh of DoD programs and projects. The IPv6 technologies to support the operational needs of this varied set of users are still being developed, especially with respect to security and mobility. The DoD faces specific challenges in the following four categories:

- Prioritizing IPv6 resources by DoD components.
- Training experienced IPv6 IT staff to support testing, operations, and maintenance.
- Availability of IPv6 capable products and advanced IPv6 features.
- Scheduling dependencies and coordinating DoD networks.

To manage the security challenges and associated risks, the DoD has established a set of milestone objectives to guide the development of information assurance security configurations and allow transition to occur only after understanding the vulnerabilities. Milestone Objective 1 provides DoD components the *authority to operate using IPv6 within approved isolated network domains* (enclaves). Milestone Objective 2 provides *authority to operate using IPv6 across cooperative multi-domain environments* (transport). Milestone Objective 3 will be reached when *Defense Information Systems Networks and DoD components' core IP infrastructures are capable of accepting, routing, and processing IPv6 protocol traffic* while providing parity to IPv4.

The DoD intends to manage transition risks in the areas of interoperability, performance, and security by a measured and controlled approach and to field IPv6 capabilities using pilot implementations and test and evaluation activities. The DoD IPv6 Master Test Plan[1] identifies 17 DoD test facilities and networks to conduct IPv6 test and evaluation. One of the DoD test networks is the Defense Research and Engineering Network (DREN). DREN provided an early DoD network IPv6 pilot implementation, primarily to support DoD IPv6 research and test requirements. Although the DREN only partially represented the DoD's complex networks, valuable lessons have been learned, including the following:

- IPv6 performance was approximately the same as IPv4 on various stress tests.
- Using defense-in-depth concepts, IPv6 security was comparable to IPv4 for Wide Area Network and site protection.
- Training requirements were minimal for personnel already familiar with IPv4.
- Most equipment at the sites could be upgraded to IPv6.

More work is required in test and pilot implementations. However, early DREN efforts and results provided an optimistic start.

Way Ahead

The DoD embarked on the journey to IPv6 in June 2003 when the DoD CIO established the goal to transition to IPv6 by fiscal year 2008. We have further refined the goal to transition our core networks to provide a service offering of IPv6 by that date, with other DoD networks, infrastructures, and applications to follow. The road map to achieve this goal is being developed now. The Defense Information Systems Agency (DISA) has developed, and is now executing, IPv6 transition plans for our core enterprise networks. DISA is integrating the IPv6 implementation schedules for other DoD component core networks

into the enterprise networks transition plans. We have developed a DoD IPv6 master test plan to coordinate all IPv6 related testing activities across the DoD and promote efficient use of DoD test and evaluation resources. The DoD has acquired IPv6 address space and is developing a DoD IPv6 addressing plan. We recognize that DoD IPv6 transition progress depends, to a great degree, on industry's transition to IPv6. The DoD continues to collaborate with industry standard's bodies to ensure DoD requirements are reflected in evolving IPv6 standards.

Effective implementation of IPv6, through synchronized planning and comprehensive testing, in concert with other aspects of GIG architecture development, will enable the DoD to achieve the net-centric vision.◆

Note

1. Can be accessed at <https://gesportal.dod.mil/sites/JITCIPv6/tewg/default.aspx?RootFolder=%2fsites%2fJITCIPv6%2ftewg%2fDocument%20Library%2f1%2fJoint%20Staff%20IPv6%20Operational%20Criteria&View=%7bA84A1771%2d0AC1%2d4003%2dB341%2dC6D8EF28FA40%7d>, but a DoD Common Access Card is required.

About the Author

Kristopher L. Strance currently serves as a senior IT analyst in the Office of the Assistant Secretary of Defense (OASD) for Networks and Information Integration (NII)/DoD CIO. He is responsible for development of DoD policy for IT and National Security Strategy (NSS) interoperability, IP convergence, VoIP, and IPv6 transition. Strance has more than 30 years of experience in IT and NSS, including policy, planning, development, programming, and operational employment. His technical and management experience includes key policy and planning positions working directly for senior government executives. Strance has a bachelor's degree in biology and chemistry from the University of New Mexico. He received his commission as an Ensign in the U.S. Navy in 1975 and was designated as a Naval Flight Officer in 1976.

OASD (NII)
DoD CIO
1851 S Bell ST STE 7000
Arlington, VA 22202
Phone: (703) 607-0249
E-mail: kris.strance@osd.mil

Continued From Page 10

those attributes critical to the realization of interoperable shared services throughout the DoD.

Way Ahead. A common infrastructure enables force capabilities to be readily networked in support of joint warfighting and operations. Interoperability of capabilities is improved when military services, agencies, and mission partners create reusable *building blocks* through the use of services. NCES is a key provider of building block services as part of the common infrastructure to be leveraged across the DoD and its mission partners in the development of information sharing capabilities.

The NCES program needs to continue working collaboratively with the DoD community to expedite the delivery of its common infrastructure services, related standards, and guidance for using its services.◆

References

1. DoD CIO. "Department of Defense Net-Centric Services Strategy." Washington: DoD CIO May 2007.
2. DoD CIO. "Implementing the Net-Centric Data Strategy, Progress and Compliance Report." Washington: DoD CIO Aug. 2006.
3. DoD CIO. "PDM III Core Enterprise Services." Washington: DoD CIO Sept. 2006.

Author Contact

Ann H. Kim
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-0940
E-mail: ann.kim@osd.mil

Carol Macha
DoD CIO
Information Policy Directorate
1851 S Bell ST STE 600
Arlington, VA 22202
Phone: (703) 602-2720 ext. 145
E-mail: carol.macha@osd.mil

Making Information Visible, Accessible, and Understandable: Meta-Data and Registries

Clay Robinson
Department of Defense Chief Information Officer Office of Information Policy

The term metadata *is often misused and misunderstood. It is important to understand the categories, multiple meanings, and value of using metadata to improve the interoperability, discovery, and utility of data assets throughout the Department of Defense (DoD). Proper use and understanding of metadata can substantially enhance the utility of data by making it more visible, accessible, and understandable. Expanded use of metadata leads to better-informed decision making, improved management of information, increased return on investment for digital asset production and publishing, improved security management, and more effective information sharing.*

The DoD Net-Centric Data Strategy requires that information assets be tagged with metadata. The concept of metadata can be confusing and many people are unclear how metadata contributes to the mandates of improved discovery, accessibility, and understandability.

There are many reasons to use metadata. First, it improves precision search for specific queries; second, it clarifies context for understanding; third, it allows identification of security classifications/controls. Expanded use of metadata leads to better-informed decision making, improved management of information, increased return on investment for digital asset production and publishing, and improved security management and information sharing. The best metadata provides a rich description of information assets so that a simple search query produces meaningful results in which a user can easily determine the usefulness of the data asset. Good metadata enables users to avoid sorting through many search responses that are not relevant because of context conflicts or file type mismatches, thereby reducing time for decision-making.

In its simplest meaning, *metadata* is information about something. The term metadata, as used in this article, refers to structured definitions that describe the properties of distinct computer data assets. *Metacard* is the term often used to describe the aggregate of metadata about a particular asset similar to the notion of a catalog card in a library. An example of metadata is the description of a music file specifying the creator, the artist that performed the song, the data created, the length of play time, album name, and the genre. Without resource metadata, portable digital music players would not be so popular due to the difficulty in creating and sorting playlists or finding particular songs. Another example may be a metacard that contains information regarding an improvised explosive device (IED) event database. The IED metacard may include details such as security classification, geographic locations covered, event type, time, point of contact for access to the data (if not already granted), etc. Metadata is much more than just keyword tags; it provides richer information. Many existing programs and applications automatically produce metadata when data is created. For example, standard commercial word processing applications produce metadata such as title, time stamp, author or creator, and type of file.

> *"Metadata can be categorized in numerous ways, but three ... are resource (bibliographic), structural, and semantic."*

Metadata can be categorized in numerous ways, but three principle categories are resource (bibliographic), structural, and semantic. Resource metadata contributes principally to visibility of an information asset. Resource metadata includes security classification, title, description, creator, publish date, and other attributes. Resource metadata is similar in concept to cards in a library catalog used to locate books. In this case, metadata helps the user locate data or services. The DoD has published the DoD Discovery Metadata Specification (DDMS) (https://meta-data.dod.mil) to define a particular type of resource metadata to support precision search.

Structural metadata is critical to accessibility and *usability*. It includes schemas and models that describe structure and formatting which are critical to interoperability and the management of databases. Going back to the portable music player example, not all devices play all audio and video file formats. Designation of file format lets a user match the file type to his device. In the case of a warfighter looking for information, he may have a desktop that is limited to the types of files (i.e. Portable Document Format or Power Point) he can view and by knowing file type or size, the user can download accordingly.

Semantic metadata helps with understandability of terms and includes shared vocabularies, taxonomies, and ontologies. Communities of Interest (COIs) usually speak in their own vernacular. Terms often have unique meanings within a given COI's context, and metadata enhances understanding of their terms. As an example, the data element or term *frequency* may relate to radio spectrum in the signals intelligence community, but *frequency* may relate to the periodicity of payments for the finance community. It is unreasonable and unrealistic to have a single meaning across the entire DoD for that term. However, within particular COIs, terms should have specific meanings. Once a user recognizes a term is from a particular community, then she can better relate to the term and understand its meaning and applicability. For several years, the DoD attempted to standardize data elements with a single common meaning across the DoD. Considering the DoD's size and broad set of communities and missions, department-wide data element standardization was not successful. The DoD now recognizes the concept of COIs and is fostering an environment for each COI to describe their vocabularies using metadata.

A number of metadata-related activities are under way throughout the DoD. To promote effective use of metadata,

the DoD has issued the DoD Net Centric Data Strategy Directive 8320.2, <www.dtic.mil/whs/directives/corres/html/832002.htm>, the DDMS, DoD Net-Centric Data Strategy Program, Decision Memorandum III, and other implementing guidance. The Defense Information Systems Agency (DISA) chairs the DoD Metadata Working Group which meets bi-monthly to address a variety of metadata topics. DISA also manages the DoD Metadata Registry and Clearinghouse as well as the COI Directory. The DoD Metadata Registry and Clearinghouse provides software developers access to data technologies to support DoD community mission applications. Through the Metadata Registry and Clearinghouse, software developers can access registered extensible markup language data and metadata components, database segments, reference data tables, and related metadata information. These data technologies increase the DoD's core capabilities by integrating common data and enterprise data services built from reusable data components. For more information on the referenced items, see <www.dod.mil/cio-nii> and <http://metadata.dod.mil>. For the DoD to successfully operate in a net-centric environment, people must understand metadata. Metadata is a key element of information sharing and interoperability. For further information, see <http://metadata.dod.mil>.◆

About the Author

Clay Robinson is associate director in the DoD CIO's Office of Information Policy where he has led the development of the DoD's Discovery Metadata Specification, which is a key component of the DoD's Net-Centric Data Strategy. Robinson has a bachelor's degree in economics from Virginia Tech.

Office of the DoD CIO
Information Policy
E-mail: clay.robinson@osd.mil
Phone: (703) 602-0937

Letter to the Editor

Dear CrossTalk Editor:
The function point analysis (FPA) described in Ian Brown's article *Controlling Software Acquisition Costs with Function Points and Estimation Tools* implies the estimating tool accepts adjusted function points (AFPs) per International Function Point Users Group (IFPUG) standard 4.2 as input and allows the estimator to perform trade-off analyses to arrive at an acceptable cost and schedule.

The FP count is backfired into equivalent source lines internal to the estimating tool. The AFP provides a single valued input, unless there is a variance associated with the FP count, which will produce a point estimate. The outputs produced in the article are all related to output distributions of cost and schedule. Point inputs produce point outputs. Are we to assume the AFP produces an input with low – most likely – and high FP counts? The article also discusses the use of commercial off-the-shelf (COTS) and reused components as part of the trade-off analysis. The use of these components in the trade-off analysis raises the zero function point problem when dealing with the cost and schedule impact associated with reused system components.

– Dr. Randall Jensen
<randall.jensen@hill.af.mil>

Dear CrossTalk Editor:
In spite of the fact that function points have been around for more than a quarter of a century now, there are still many misconceptions and misunderstandings about function points. Let me address each point in turn.

First, most estimation tools accept unadjusted function points as a sizing input. The tools rely on more targeted parameters such as multiple site development, reuse required, and requirements volatility to calculate estimation adjustments that might have been handled by the general systems characteristics and AFPs before parametric tools were as prevalent as they are today.

Second, function points are but one input into an estimation tool. Other cost drivers, such as personnel capabilities and experience, development environment, and product requirements are used to tailor the cost estimate to the particular program. Very often these parameters are expressed as ranges – particularly in an acquisition environment where specific information may not be available. For example, the program office may have a minimum Capability Maturity Model® Integration level required for the vendor, which would set a minimum level for some of these parameters. But some vendor may bid that performs well above that level, so the acquisition cost framework should include a range of inputs to account for this possibility. When any of the input parameters are set as ranges, the estimation tool will produce a range of cost and schedule outputs. That being said, Dr. Jensen does bring up an excellent point: the function point count itself may be expressed as a range (low, likely, and high). The acquisition process may be in such an early stage that requirements may not be fully defined, or there may be some uncertainty associated with system functionality. In this case, it is completely appropriate to use a size range to develop the acquisition cost and schedule framework.

Finally, let's talk about the *zero function point problem*. Function points measure software size independent of language, technology, or platform – and that includes COTS and reused components. If I've got a set of requirements that translates into 500 function points, and I decide to use a COTS product to meet half of those requirements, I've still got system that is 500 function points in size. It did not all of a sudden just become 250 function points. I would simply have to model the effort differently in the estimation tool than I would if all requirements would be custom developed. I would need to make sure that I knew how to reflect these differences appropriately in the parametric model. This is why you need an experienced person working with the tool. A fool with a tool is still a fool – these tools are powerful and flexible enough that you can get all kinds of answers out of them, and the trick is understanding if you've got the inputs set up right.

– Ian Brown
<brown_ian@bah.com>

® Capability Maturity Model is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

Managing the Air Waves: Dynamic Spectrum Access and the Transformation of DoD Spectrum Management

Thomas J. Taylor
Office of the Assistant Secretary of Defense

The electromagnetic spectrum is a finite resource that enables the first tactical mile of the Global Information Grid. From radars that gather information, to networks that transfer the information and targeting for precision guided munitions; the electromagnetic spectrum is a critical resource that enables us to do more with less human capitol. Along with the Department of Defense's (DoD) increase in dependency on this resource, the commercial sector is also increasing its requirements for more and better spectrum access. As a result, the DoD is transforming its electromagnetic spectrum management capabilities to meet future demands.

The DoD is in the process of transforming its legacy spectrum management processes and capabilities to address the ever changing Global War On Terror and provide for net-centric military operations. This transformation envisions assured access to spectrum by warfighters anytime and anywhere, a prerequisite for the untethered, reliable, and ubiquitous wireless networking component of net-centric operations. To fully realize this vision, the DoD has focused on developing net-centric spectrum capabilities to help us plan and manage the following:

- On-the-move dynamic operations (which also require environmental awareness).
- Sustained growth of spectrum requirements by the DoD systems.
- Emerging commercial wireless systems and requirements for additional spectrum.
- Flexible policies and processes to support global deployments.
- Complete life-cycle, end-to-end, spectrum supportability processes and tools.

In response to challenges in operational, technical, and regulatory areas, the DoD spectrum community is updating spectrum management strategic plans and policies that will guide the transformation of DoD spectrum access. In 2006, the DoD stood up the Defense Spectrum Organization (DSO), which combines the Joint Spectrum Center (JSC) and the Defense Spectrum Office, to become the center of excellence for spectrum under Defense Information Systems Agency (DISA). The new organization is responsible for developing the comprehensive and integrated spectrum plans and long-term strategies to help DoD rise to the challenge. Additionally, the DSO provides the operational support center required by joint commands to meet their global missions.

The most important element of this transformation includes the development of improved tools, data systems, and services that support the entire range of spectrum activities including strategic planning acquisition support and mission operations. This capability is captured by a new system called the Global Electromagnetic Spectrum Information System (GEMSIS). The GEMSIS program will develop a suite of capabilities that will improve spectrum deconfliction in the operational environment, enhance integration of frequency assignment processes with mission planning, develop new spectrum services for the acquisition community, and provide the policy for dynamic spectrum access (DSA).

In order to achieve global access to spectrum for our networks in the new operating environment, DSA has emerged as a capability that has the potential to effectively address network spectrum resource challenges by allowing more dynamic, flexible, and autonomous spectrum access. DSA is realized through wireless networking architectures and technologies that enable wireless devices to dynamically adapt their spectrum access according to criteria such as policy constraints, spectrum availability, propagation environment, and application performance requirements. The basic concept of DSA is that spectrum-dependent systems can dynamically change their parameters to access multiple dimensions of the spectrum resource including frequency, space, time, and signal codes. This agility, coupled with enhanced distribution of spectrum data directly to spectrum-dependent systems, will enable these systems to share in near-real time the spectrum resource among a large number of users, improving the utilization of spectrum. Transforming from the current static spectrum allocation to DSA is analogous to the paradigm shift from the circuit-switched to packet-switched networking, where significant efficiency gain and improvement in interoperability can be realized.

DSA can be broadly classified into two categories: coordinated DSA and opportunistic DSA. Coordinated DSA requires a spectrum control and management infrastructure. One envisioned concept utilizes a set of control nodes (spectrum brokers) that are responsible to dynamically allocate spectrum within a geographical area to support a group of users. Opportunistic DSA adopts a distributed model where a group of devices autonomously sense the environment and access spectrum according to pre-defined policies. The system developed under the Defense Advanced Research Projects Agency XG (next generation) program implements an opportunistic approach to DSA. Regardless of form, DSA systems will require new data and knowledge representation constructs and software-based autonomous processing capabilities.

Effective DSA requires the full breadth of spectrum management to be brought to bare. First, the DoD must identify the spectrum bands that provide the best opportunity for global use from an environmental density perspective and a regulatory perspective. This can only be accomplished through the robust modeling and simulation of the electromagnetic environment that is envisioned in GEMSIS. Once the environment is defined, then the new DSA equipment must be supported through policy agreements both internationally and nationally. Accomplishing DSA-enabled networks is no small task and will require close partnership with industry and the DoD.

DSA-enabled networks can provide warfighters with improved net-centric performance globally. By integrating DSA with the other elements of DoD spectrum transformation assured spectrum access will enhance battlefield management of the electromagnetic environment and improve military operations in the net-centric environment.◆

About the Author

Thomas J. Taylor is responsible for the policy, oversight, and guidance of the Spectrum Management Warfighter Integration.

Phone: (703) 607-0726
E-mail: thomas.taylor@osd.mil

Trusting the Team: Identity Protection and Management

Defense-Wide Information Assurance Program

Identity protection and management is at the heart of establishing and maintaining a secure and interoperable infrastructure. We must be able to trust the identity of information producers, service providers, and consumers of the information and services. The article highlights the Department of Defense's (DoD's) primary initiatives in this area.

Information superiority is heavily dependent on establishing and maintaining a secure and interoperable infrastructure. At the heart of it all is identity protection and management. We must be able to trust the identity of information producers, service providers, and consumers. In pursuing these objectives, many goals over the past 15 years have been achieved, primarily through the efforts of three DoD initiatives: Common Access Card (CAC), Public Key Infrastructure (PKI), and biometrics.

The CAC provides the standard identification card for authorized DoD users – the DoD credential enabling physical and logical access. The DoD has issued more than 11 million identity cards (more than 3.5 million are in current circulation). Use of the CAC and the PKI certificates on the token eliminates the need to use passwords when authenticating. This mitigates a major problem with protecting DoD networks from unauthorized intruders.

In addition to improving the security of our networks, the CAC, with its PKI credentials, is also accelerating our migration to the Web. By allowing the use of digital signatures in systems like the Defense Travel System, labor-intensive paper processes are being eliminated. The CAC also provides the means to improve physical access security at DoD installations around the world. When a base or a theater of operations implements rapid electronic authentication, hundreds of fake identification cards are confiscated every week and unauthorized accesses are prevented (more than a million in Europe alone in just one year). Our DoD CAC initiative is one of the most award-winning and successful smart card efforts in the world.

PKI utilizes a combination of software, encryption technologies, and services that enable enterprises to protect their communications and business transactions on networks. PKI integrates digital certificates, public-key cryptography, and certificate authorities into a total enterprise-wide network security architecture. The DoD has initiated one of the largest PKI implementations in the world with more than 20 million certificates issued across the DoD. Since the mandate to move to cryptographic log-in on our networks, the DoD reduced successful intrusions into its networks by 46 percent.

Biometrics provide a measurable identity factor that can be bound to an electronic identity for use during authentication. Measurable physiological or behavioral characteristics – including fingerprints, iris recognition, voice analysis, and handwriting dynamics – can be used to validate an established identity. In 2006, the Deputy Secretary of Defense established the defense research and engineering as the Principal Staff Assistant for Biometrics and the Army established the Biometrics Task Force to lead, consolidate, and coordinate all biometric information assurance activities and ensure biometrics technologies are integrated across DoD. Every day in Iraq and other area of responsibility sites, biometrics of visitors and workers are being checked against terrorist watch lists and Red Force databases. We are detaining people whose fingerprints were left behind on improvised explosive devices and denying access to those individuals on these watch lists.

To align the efforts of these three program offices into one coordinated venture across the DoD, the Identity Protection and Management Senior Coordinating Group (IPMSCG) was established in January 2004. The IPMSCG oversees DoD policy, strategy, and capability implementation and has developed the DoD Road Map to Identity Superiority. Also critical in the Global War on Terror is the need to align these DoD efforts with similar initiatives within the federal government, law enforcement agencies, state and local governments, and allied coalition forces.

Homeland Security Presidential Directive No. 12 <www.whitehouse.gov/news/releases/08/20040827-8.html> establishes the framework for a common identification standard for all federal government employees and contractors. The standards-based credential will facilitate electronically validated entry to federal facilities and electronic credential-based authentication to virtual spaces, enabling more secure information sharing within the federal government. To meet these requirements, the DoD's pursuit of next-generation identity-based technologies, standards, and processes must include such key elements as the following: identity proofing, credentialing, directory services, authentication, authorization, privacy, and a tighter link between the identity proofing and credentialing processes.

Identity Superiority

As detailed in the DoD Road Map to Identity Superiority, the success of the DoD's approach to identity management is crucial if we are to advance to a broader, next-generation identity protection and management capability or identity superiority. Identity superiority will enable *secure*, *integrated*, *interoperable*, and *scalable information sharing solutions* for people, systems, and services in a net-centric warfare environment. In implementing the DoD's approach to identity superiority, a number of initiatives that take advantage of CAC, PKI, and biometrics are under way:

- Mandated use of the CAC to log-on to DoD networks decreases the use of passwords, significantly decreasing successful DoD network intrusions by 46 percent and socially engineered email attacks by 30 percent.
- DoD Interoperability Root Certificate Authority is being established (~March 2007) as a first step in enabling the DoD to have the ability to successfully interoperate with non-DoD entities (on a limited basis).
- Automated Biometric Identification System is currently a repository of Red Force biometrics data. This data is used in identifying potential national security threats.

There is still significant work that needs

to be done. Achieving identity superiority requires more than the efforts of the three program offices. Actions required to achieve identity superiority include aligning initiatives under way in each of the three program offices, expanding the focus to accommodate the continually evolving warfighting environment, and identifying additional enabling processes and technologies that are needed but not yet supported. Identity is key to being able to take full advantage of the power of the Internet.

With a well-defined and trusted identity management architecture, the DoD can evolve its current access control model to where consumers with authorized credentials can access information without having to pre-register with the information provider. For this evolution, the DoD is pursuing the concept of Attribute Based Access Control; where policy-based, fine-grained access control processes use validated attributes to authenticate users and devices and make authorization decisions. Attributes are qualities or characteristics inherent in or ascribed to an identity (human or device) such as mission, function, area of interest, name, rank, role, citizenship, location, or organization. This is the new direction of authorization needed for information sharing. It is the combination of *identity*, knowing who you are, and *information release* – knowing who can see a piece of information. Authorization is the process that joins these two pieces of knowledge together.

The DoD has long emphasized using state-of-the-art technology to secure and protect its most vital assets: people, information, and equipment. Our quest for identity protection and management or identity superiority will continue that tradition and provide our warfighters and supporting workforce with the enabling technology and tools necessary for tomorrow's challenges.◆

About Defense-Wide Information Assurance Program

This article was a combined effort of several members of the Defense-Wide Information Assurance Program (DIAP). The DIAP is within the Information Assurance Policy Directorate of the Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD [NII]) DoD Chief Information Officer (CIO) and is responsible to the ASD (NII) DoD CIO for ensuring Information Assurance (IA) is pursued and implemented throughout the DoD, as well as the intelligence community, as a critical operational readiness issue. The DIAP Office coordinates, integrates, and oversees IA processes of the DoD and is the central focal point for organizing and marshalling the resources to execute its mission. The program's operations are focused on linking and integrating IA management into the DoD planning, programming, budgeting, and execution process; the requirements generation process, the acquisition process, and readiness reporting process. More information on the DIAP can be found at <www.defenselink.mil/cio-nii/infoassurance/diap/index.html>.

Communicating on the Move: Mobile Ad-Hoc Networks

Robert F. Dillingham
SRA International, Inc.

Dean Nathans
Office of Secretary of Defense

Mobile Ad-Hoc Networks (MANET) is wireless networking that continually re-organizes itself in response to its environment without benefit of a pre-existing infrastructure. A MANET is comprised of a set of mobile participants who must communicate, collaborate, and interact in order to complete an assigned mission. The challenges of MANET are to provide wireless, high-capacity, secure, and networked connectivity. Participants must communicate using bandwidth limited wireless links, with potential intermittent connectivity, as compared to stable wired links and infrastructure. MANET is a key enabler for achieving the goals of net-centric operations and warfare, provides the right information at the right place at the right time, and shortens the kill chain by extending the Global Information Grid (GIG) to the tactical edge.

The Internet is dominated by wired network technologies in which dedicated devices perform the task of forwarding data from source to sink. Wireless attachments to the network are handled through fixed access points that convert wireless data to wired data and vice versa. The GIG expands on the Internet architecture with the addition of airborne wireless, as well as space-based components in its transport layer. Both networks employ the Internet Protocol (IP) suite.

Military MANET must accommodate a diverse mix of deployed units, platforms, and systems with critical communications needs, often in adverse environments. At times, operation may be autonomous or connections may be through the space or wired networks, but the expectations are that networking services will continue without interruption. The entire network or portions of it may be mobile and subject to outages or losses inherent in a military environment. Therefore in a MANET, every node must be capable of forwarding data packets destined for other nodes. Forwarding decisions must be made independently by every node based on some combination of function, sensed network connectivity, and previously shared routing information.

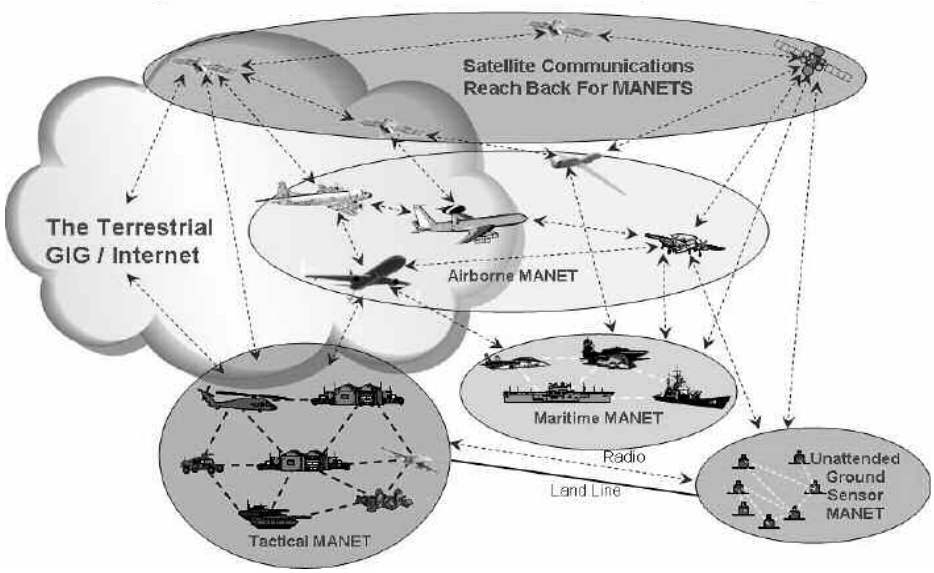
MANETs are found in several major developmental military communications programs; the most visible of which are the Army's Future Combat System, the Army's Warfighter Information Network – Tactical (WIN-T), the Joint Tactical Radio System (JTRS) and space borne Transformational Communications which includes the Transformational Satellite Communications System and Mobile User Objective System programs.

MANET Capabilities/Challenges

The challenges of implementing effective MANETs are exacerbated in the military environment. MANETs must be developed to accommodate numerous and diverse missions ranging from formations of soldiers to high-speed aircraft communications. Some of the resulting challenges of particular significance in the military environment include the following:

- **Interoperability.** To be interoperable, DoD MANETs must be developed within a consistent, integrated architecture, with defined hierarchal relationships, network structures, and GIG attachment points. The DoD is developing this interoperable architecture with various DoD level and service/agency efforts defining the net-centric architecture and interfaces. At lower network layers, channel access methods, operating frequencies, and security techniques must all be compatible or no link can be established. At mid-layer machine to machine authentication, routing/addressing and networking services must work together to implement the IP suite. At the highest networking layers, message formats and applications must all be compatible to provide the user a comprehensible output. Figure 1 illustrates the highest levels of interoperability and hints at the complexity of the problem.
- **Mobility Support.** The mobility aspect of MANETs has significant ramifications. At the physical layer, motion places an additional burden on the radio receivers in the form of Doppler shifts, signal outages due to body shading or terrain, range and multi-path; all contributing to link instability. Since nodes are free to move randomly, MANET is differentiated from wireless ad hoc networking by a heightened sensitivity to time.
- **Discovery.** In ad-hoc networks, nodes do not have a priori knowledge of the network around them. A node (optionally) announces its presence and listens to broadcast announcements from its neighbors. This activity is generally termed *neighbor discovery*. The process of neighbor discovery must be continuous (at some predeter-

Figure 1: *Top Level MANET Interoperability*



mined rate) in order to maintain current knowledge.

- **Network Management.** Many areas fall within the realm of network management including IP configuration, security, spectrum, monitoring, and reconfiguration upon loss of nodes. Minimal configuration and quick deployment make ad hoc networks desirable for those in direct military conflict. There must be coordination among nodes to accomplish network management, while the ad-hoc nature of MANETs makes this coordination more difficult. MANET network management schemes must also be interoperable with higher level planning and network management layers.
- **Routing/Scalability.** If we add the advantage of a flawlessly interoperable communications infrastructure, how big a MANET is reasonable? It is well established that radio frequency spectrum available to MANET is limited, directly affecting information transfer capacities. At a minimum, MANET must perform neighbor discovery and collect extended neighborhood awareness information to maintain a local picture of network topology. Topology sustains routing. The amount of network traffic required to maintain topology varies with each MANET approach and the needed overhead increases as the number of nodes increase. Changes in the (MANET) network trigger additional topology maintenance traffic, consuming capacity. Based on field testing and limited modeling and simulation, current estimates of the size of a MANET network generally fall into the 10 to 200 node range. These numbers are based on early field data collected during Defense Advancement Research Projects Agency, Army, and Air Force experimentation augmented by a large body of modeling and simulation.
- **Security.** Security is a matter of life and death in combat and sets the military apart in many respects from the commercial world. Elements needed for security consume information capacity and add both design and operational complexity and cost. For example, the basic question of exposure. For a node to be discovered it must broadcast. Therefore it can be located, tracked, and potentially compromised. Covertness is achieved through low observable transmission techniques or by ceasing to transmit altogether, both of which have adverse affects on MANET network awareness. On the other hand, when a node is actively transmitting and receiving, authentication and data encryption are required at a minimum, impacting overhead loading.
- **Layered Interaction.** Each layer of the protocol stack plays an important part in the overall communications process for a MANET. An effective MANET solution addresses all layers of the protocol stack; single mechanisms at particular layers can mitigate particular technical issues but not the general MANET problem space. Interaction among network layers in MANETs improves overall functionality.

Outlook

The development of DoD MANETs present significant challenges and much development effort remains, however solid progress is being made. The JTRS and WIN-T programs have demonstrated increasing capabilities with early versions of their networking waveforms. The Office of the Assistant Secretary of Defense (Networks and Information Integration) (OASD [NII]) DoD Chief Information Officer continues to refine guidance and direction to provide a cohesive basis for an interoperable architecture. This process will be a continuing one as DoD capitalizes on emerging technology to improve on current solutions.◆

About the Authors

Robert F. Dillingham is a member of the senior technical staff at SRA International, Inc., and has more than 28 years of research, development, test, and evaluation experience in navigation, guidance and control, command and control, communications, and software simulation/hardware emulation. He has extensive experience in the design, specification, implementation, and operation of laboratory and test facilities with specific expertise in the areas of global positioning software (GPS), real-time systems, networking and embedded applications. Dillingham provides review and comment on behalf of JTRS10 on the series of documents in process by the JTRS Joint Program Executive Office, and the Joint Network Enterprise Services working group, which is defining common network and enterprise management services. Prior to SRA, he was a civilian employee of the Navy, where he was the lead systems designer for the Navy GPS Central Engineering Activity, and systems engineer for the first GPS satellite signal generator. Dillingham has a bachelors degree in electronics engineering from Lehigh University.

101 E County Line RD STE 300
Hatboro, PA 19040
Phone: (215) 672-8005 ext. 114
Fax: (215) 672-8708
E-mail: robert_dillingham@sra.com

Dean Nathans is the senior staff assistant for Military Satellite Communications (MILSATCOM) Terminals in the Communications Directorate, OASD (NII) where he is responsible for oversight of microwave communications satellite terminal programs and for providing technical advice for MILSATCOM, JTRS and Mobile Ad-Hoc networking programs. He has been involved with the development of military communications and navigation systems for more than 25 years. Prior to assignment at OASD (NII), Nathans was a deputy program manager in the ground-based mid-course command, control, and communications (C3) Program Management Office at the Missile Defense Agency. Nathans has a masters degree in electronics engineering from Villanova University and a bachelor's degree in electrical engineering from Rutgers College of Engineering. He has received several awards for his service, including the Navy Meritorious Civilian Service Award and is a registered Professional Engineer.

OASD (NII)
DASD (C3, Space andSpectrum)
Communications Directorate
6000 Defense Pentagon
Washington, D.C. 20301
Phone: (703) 607-0263
Fax: (215) 607-0276
E-mail: dean.nathans@osd.mil

Reconfiguring to Meet Demands: Software-Defined Radio

Dean Nathans
Office of Secretary of Defense

Dr. Donald R. Stephens
Joint Program Executive Office

A Software Defined Radio (SDR) allows a single hardware platform to be reconfigurable so that it can accommodate multiple radio waveforms and be easily upgraded with software changes. The Joint Tactical Radio System (JTRS) is the Department of Defense's (DoD) solution for a family of tactical SDRs based on common open standards and architectures. JTRS accommodates legacy and new mobile ad hoc networking waveforms. Additionally, military Satellite Communication, and Intelligence, Surveillance, and Reconnaissance (ISR) terminals are migrating to SDRs to enable consolidation of multiple legacy systems into single multi-band configurations. This article describes current military SDR programs, their challenges, and the way ahead for the DoD.

Current communications systems have evolved to meet service specific and mission specific requirements. Specialized functionality has resulted in limitations in communicating from one system to another resulting in interoperability issues. More recent DoD systems such as Link-16[1] have made large strides in providing more capable and interoperable data links; however, the DoD must now evolve to acquire a family of high capacity, interoperable, networked, and affordable radio systems as part of the transport layer of the Global Information Grid (GIG).

The appeal of SDRs is the ability to handle multiple radio communication protocols on a single hardware platform by means of programmable hardware controlled by software. From a DoD perspective, the reprogrammable radio can store and run multiple waveforms. Rather than developing many different radio systems operating to different standards, SDRs enable the DoD to have a family of interoperable radios based on common waveforms, standards, and interfaces.

For the DoD, the impetus for SDRs is to significantly reduce the number of different radios and waveforms in the inventory. Hand in hand with these reductions is the elimination of proprietary or unique implementations, eliminating interoperability issues. Costs to the DoD for radio systems are also significantly reduced, and SDRs contribute to net-centricity by enabling newer high-rate, networked waveforms.

DoD SDR Programs

Trying to develop a reduced set of radios and waveforms for the DoD generates challenges in itself as the family must accommodate numerous requirements from each service. Software flexibility provides the ability for operation of many waveforms on single hardware platforms; however, there are still many additional unique military challenges. The radios must be useful in air, sea, and ground applications with different size, weight, power, environmental, and threat needs.

To develop a family of radios useful to all services, the Joint Tactical Radio System (JTRS) Program was initiated in 1997. Initially, waveforms and cryptographic applications were controlled by the JTRS Joint Program Office, and JTRS hardware development was assigned to service leads. The DoD recently restructured the program so that all JTRS products would be under the control of the Joint Program Executive Office JTRS (JPEO JTRS). JTRS programs currently include Ground; Airborne, Maritime, and Fixed Site (AMF); and Network Enterprise Domains (NED). The ground domain includes ground vehicular, Manpack radio, handheld, and special applications. The AMF domain includes standard airborne, Multifunctional Information Distribution System – JTRS, and 19-inch rack applications. The NED includes the waveforms, gateways, and common networking services products used by the other domains. Included within the NED programs are new networking waveforms based on Internet Protocol (IP) standards that allow interoperability and include Mobile Ad-Hoc Network (MANET) protocols for operation over bandwidth constrained and potentially intermittent wireless links.

"The JPEO is developing and implementing a common infrastructure across all domains to define a host environment that ensures a waveform porting among JTR sets."

The JPEO is developing and implementing a common infrastructure across all domains to define a host environment that ensures waveform porting among JTR sets. The hardware domains have been partitioned to allow common core hardware and software in each domain, which is then tailored with additional modules to apply to its unique applications. To ensure waveforms are portable and perform as intended, they go through a rigorous certification process under the auspices of the JPEO.

The foundation for the JTRS family of radios is the Software Communications Architecture (SCA), Figure 1 [1]. It is simultaneously an architecture framework, specification, and guidance document for software defined radios allowing convenient reuse, update, or replacement of software. The JPEO JTRS currently has over 3.5 million source lines of SCA compliant code in its Information Repository (IR) [2] developed by the JTRS community. When a new JTRS program requires software, the program developers download it from the IR, which enhances interoperability of JTR sets, since all instantiations are based upon the same software.

To further support waveform portability and code reuse, the SCA specifies operating system Application Programming Interfaces (APIs) that must be provided by the JTR set's Real Time Operating System (RTOS). Labeled the Application Environment Profile (AEP) in Figure 1, the SCA specifies a subset of

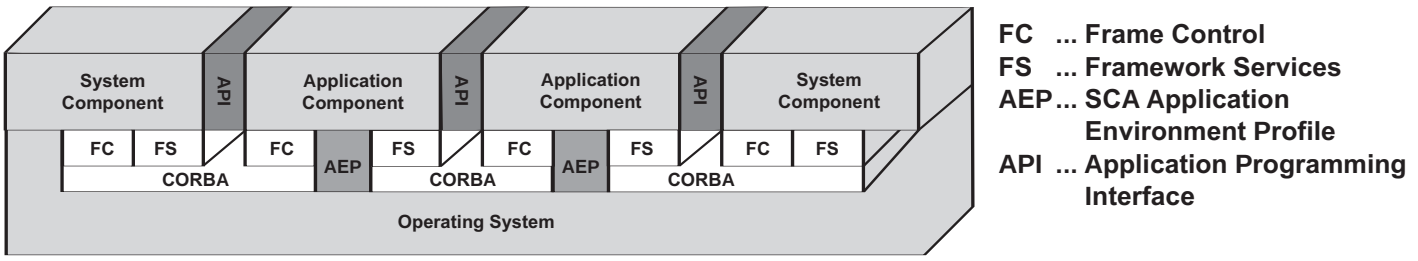


Figure 1: *SCA Component Architecture*

the Portable Operating System Interface that every JTR set must support and to which each waveform is limited. In combination with the defined Common Object Request Broker Architecture middleware, the SCA guarantees that every SCA-compliant object can be executed upon any JTR set.

Originally, JTRS was envisioned to cover the entire radio spectrum. However, during the JTRS restructure, the DoD determined that satellite communications and line-of-sight radios operating in the Super High Frequency (SHF) and the Extremely High Frequency (EHF) spectrum have a large enough set of distinct features and requirements to keep them separate from the JTRS Program. One of the largest differences is the high throughput demands of some of the SHF and EHF waveforms. In addition to JTRS, the DoD has continued with a set of multi-band SHF/EHF terminal SDR programs led by the services. These SHF/EHF programs invoke the JTRS SCA; additional collaborative possibilities, including a common reference architecture, are being pursued.

SHF/EHF Programs include the following:

- Air Force Family of Advanced Beyond Line-of-Sight Terminals.
- Army High Capacity Communications Capability.
- Army Joint Command, Control, Computers ISR (JC4ISR).
- Multi-Role Tactical Common Data Link Demonstration Program.
- Navy Multi-band Terminal.

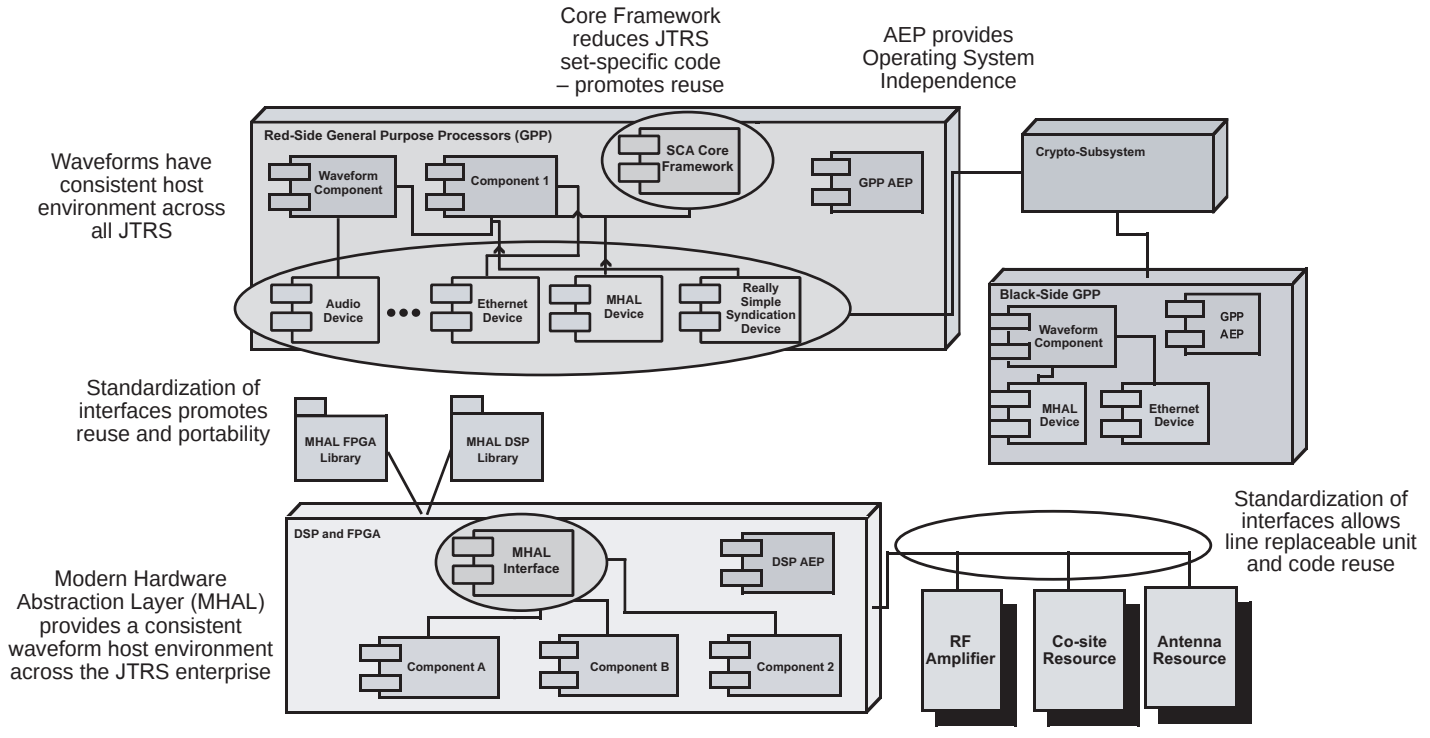
JTRS Enterprise Architecture

JTRS is a family of radios which spans across multi-channel, vehicle-mounted radios to disposable, unattended ground sensors. Although early expectations might have been for one software suite that could be installed into any radio, it is not practical to deploy radios with capabilities exceeding their missions. Individual JTR sets are expected to reuse as much host environment software as possible from the JTRS information repository, but are permitted to integrate unique implementations of devices and services as long as the JTRS APIs are supported. The set provider's primary responsibility is to meet mission requirements. Waveform software is expected to be largely consistent across all JTR sets.

To achieve interoperability and software reuse, the JTR set providers are required to provide set-to-waveform interfaces that are consistent across the JTRS enterprise [3]. The JTR set implementations of components may be unique, but the exposed interfaces to the waveforms are standardized. Figure 2 shows the deployment of the JTRS infrastructure.

The infrastructure defines the host environment for all JTRS software components. A software component in an unattended ground sensor has exactly the same operating system functions, the same middleware communication, and the same hardware interfaces as a software component deployed in a multi-

Figure 2: *Deployment of the JTRS Infrastructure*



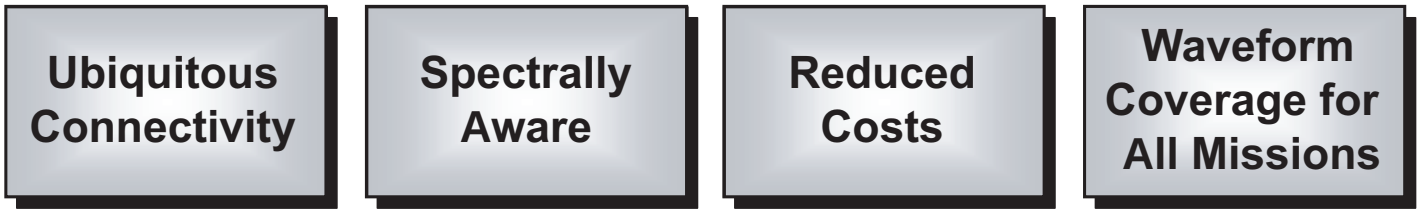


Figure 3: *Evolution of SDRs*

channel vehicle-mounted radio. Regardless of whether the software component is a general purpose processor, Digital Signal Processor (DSP), or Field Programmable Gate Array (FPGA) component, the JTRS infrastructure further defines a host environment that is consistent across the enterprise. Implementations may vary due to the mission or size, weight, and power requirements, but the host environment and the exposed radio services and hardware interfaces are the same.

JTRS SCA and Enterprise Architecture Future Increments

The JTRS infrastructure of Figure 2 has resulted in an executable and sustainable deployment model for the JTRS family of radios. The requirements for the next increment of JTRS are still in development, so it is early to conjecture about the feature set of the next-generation JTRS infrastructure. Because the information repository will have approximately four million lines of source code from JTRS Increment 1, it is probable that the future infrastructure must be backward compatible with today's infrastructure.

As additional form factors are developed, there may be minor revisions to the SCA to extend the current architecture. To better support battery-powered missions, there may be specific changes to the RTOS and middleware specifications. In addition, System on Chip (SOC) interconnection is becoming increasingly important and standardization may be required because FPGAs have become capable of hosting increased functionality of the SDR.

SDR Challenges

Because of the complexity of SDRs, systems and software engineering is more important now than for the previous generation of radios. Developers in both the commercial and DoD sectors must ensure sufficient training and experience necessary for SDR development including engineering disciplines of communications systems, radio frequency, digital/analog hardware, software, and digital signal processing. Complementing a need for developer training is the requirement for improved development and test tools. Recognizing the need and potential marketplace, several companies have emerged specifically targeting SDR development tools. A key item in achieving waveform reuse is the use of compatible tools with thoroughly documented code.

An additional challenge for the SDR developer is to design the architecture such that interfaces may be replaced with a different standard at a future date. The selection of a set of open standards among many competing standards is also a challenge for DoD in achieving more reuse of hardware and software among programs.

"SDRs will be able to handle new networking waveforms, while also being able to operate prior legacy waveforms so that interoperability can be maintained as the older waveforms are phased out."

Hardware innovations and improvements are required for SDRs to achieve their full potential. Greater performance can be achieved with improved analog to digital (A/D) and digital to analog (D/A) converters; reduced power parts, especially FPGAs; wider bandwidth and more linear amplifiers; and radio frequency (RF) technology allowing wider bandwidth operation. For SHF/EHF systems, improvements are needed to reduce the high costs of the steerable, directional, antenna systems.

A unique challenge for DoD is that radio life cycles are three to 10 times longer than commercial products. The life cycle was less problematic with hardware defined radios, but SDRs utilize commercial products such as operating systems, middleware, and software development tools. DoD platforms such as aircraft carriers, aircraft, submarines, etc., have very long life cycles. SDRs represent an opportunity to update the communications capabilities in these platforms for relatively low cost.

Evolution of DoD SDRs Into the Future

SDRs will continue to play a larger role in allowing military users to seamlessly interoperate and provide the wireless interface to the GIG. In addition, SDRs will help reduce the total number of radios in the DoD inventory, allow fielded systems to be more easily refreshed and upgraded, and help with the drive towards a reduced number of waveforms and protocols. SDRs will be able to handle new networking waveforms, while also being able to operate prior legacy waveforms so that interoperability can be maintained as the older waveforms are phased out. The evolution of SDRs is shown in Figure 3.

Ubiquitous Connectivity

The next increment of SDRs must continue the paradigm shift from a communications model of disparate, service-owned and operated radio communications to net-centric warfare by unifying communications resources that are shared across cooperating services. The current increment of JTRS is evolving the radio and networking technologies necessary to realize this vision. Net-centric warfare integrates mobile/tactical users via networked IP and meets frontline demands for bandwidth. The next generation transport architecture will include routers and translation services to enable meaningful and seamless connectivity between multiple, diverse tactical and theater networks and satellite resources. SDRs must incorporate frequency reuse mechanisms to maximize use of available spectrum.

Spectrally Aware

Frequency bandwidth is required to supply the warfighter with the information needed for tomorrow's battlefield. Unfortunately there is a dearth of unassigned frequency spectrum and without simultaneous regulatory and technology breakthroughs, radio spectrum will become a limiting resource for the DoD. A potential reuse mechanism is a spectrally aware radio that is trusted by regulatory agencies to monitor the frequency spectrum and only transmit in unused frequencies.

Reduce Costs

The JTRS program has consolidated multiple radio domains under a single program executive office. Through the use of a common infrastructure, the JTRS JPEO is maximizing reuse of products through its enterprise and correspondingly reducing development and procurement costs. Additionally, a core set of interoperable networking waveforms is being developed. Currently, the DoD is continuing with individually managed service multi-band SHF/EHF programs; however, future collaborative possibilities are being examined. Reuse of the SCA and some of the JTRS enterprise architecture is anticipated, with additions as needed to establish an SHF/EHF reference architecture.

Waveform Coverage for All Missions

Communications for DoD missions vary from dismounted soldiers in the canyons of Afghanistan, supersonic aircraft, unattended ground sensors in the tropics, to conventional office environments. Although one waveform for all communications would be desirable, it is as impractical as expecting that all DoD transportation needs can be served with a single vehicle. The next increment of SDRs will provide coverage of all DoD communication needs with fewer waveforms.

Outlook

The development and use of SDRs is a key enabler for DoD in achieving a family of interoperable radios based on common waveforms, standards, and interfaces, with enhanced portability and reusability. While there have been significant developmental challenges, the DoD SDR programs have made good progress, with prototypes available and being tested in the field for several JTRS and SHF/EHF programs. As users gain familiarity and experience with these radios, their transformational communications capabilities will become evident. The reprogrammable SDR will allow further evolution to additional advanced capabilities building upon the current programs.◆

References

1. JTRS-5000SCA. "Software Communications Architecture Specification (SCA)." V2.2.2. 15 May 2006.
2. North, R., N. Browne, and L. Schiavone. "Joint Tactical Radio System – Connecting the GIG to the Tactical Edge." Military Communications (MILCOM), 2006.
3. Stephens, D.R., B. Salisbury, and K. Richards. "JTRS Infrastructure Architecture and Standards." MILCOM, 2006.

Note

1. Link-16 is a secure near real-time situational awareness and command/control data link used on the Joint Tactical Information Distribution System and Multifunctional Information Distribution System Terminals of the United States and North Atlantic Treaty Organization allies.

About the Authors

Dean Nathans is the senior staff assistant for Military Satellite Communications (MILSATCOM) Terminals in the Communications Directorate, Office of the Assistant Secretary of Defense for Networks and Information Integration (OASD [NII]) where he is responsible for oversight of microwave communications satellite terminal programs and for providing technical advice for MILSATCOM, JTRS, and Mobile Ad-Hoc networking programs. He has been involved with the development of military communications and navigation systems for more than 25 years. Prior to assignment at OASD (NII), Nathans was a deputy program manager in the ground-based midcourse Command, Control, and Communications (C3) Program Management Office at the Missile Defense Agency. Nathans has a masters degree in electronics engineering from Villanova University, and a bachelor's degree in electrical engineering from Rutgers College of Engineering. He has received several awards for his service, including the Navy Meritorious Civilian Service Award, and is a registered Professional Engineer.

OASD (NII), DASD
(C3, Space and Spectrum)
Communications Directorate
6000 Defense Pentagon
Washington, D.C. 20301
Phone: (703) 607-0263
Fax: (215) 607-0276
E-mail: dean.nathans@osd.mil

Donald R. Stephens, Ph.D., is JTRS standards manager at the JPEO JTRS, San Diego, CA. His team is responsible for the establishment and standardization of the JTRS infrastructure. Stephens has development experience with three software radios: the Digital Modular Radio, the Joint Tactical Terminal, and the Airborne Integrated Terminal Group. He has extensive experience in multiple communications and radar receiver systems including satellite communications, spread spectrum waveforms, and multi-spectral signal processing with companies such as Raytheon E-Systems, McDonnell Douglas, Emerson Electric, and Scientific Atlanta. Stephens has participated in all technology facets of software radio design such as RF, DSP, distributed computing, security, and networking. He authored *Phase-Locked Loops for Wireless Communications: Digital, Analog, and Optical Implementations* and several other publications and patents. Stephens has bachelor's and master's degrees in electrical engineering from Georgia Tech, and a doctorate in electrical engineering from the University of Missouri – Rolla.

JPEO JTRS
33000 Nixie WY
San Diego, CA 92147
Phone: (727) 642-9669
Fax: (619) 524-4522
E-mail: donald.stephens1.ctr@navy.mil

Sharing Information Today: Maritime Domain Awareness

Michael Todd
Defense Information Systems Agency

In a world where unforeseen human or natural disasters (i.e., U.S.S. Cole, September 11, Hurricane Katrina, the 2004 Indian Ocean tsunami, and the possibility of an avian flu pandemic) may occur, interagency information sharing and collaboration is essential to mitigating effects of these types of catastrophic events. The Maritime Domain Awareness Data Sharing Community of Interest (MDA DS COI) pilot demonstrated a net-centric data sharing capability as a first step towards addressing the common challenge of global identification and tracking of maritime vessels, cargo, and crew usage of existing information sources to better secure our coasts, ports, and waterways. This Department of Defense (DoD), Department of Homeland Security (DHS), and Department of Transportation (DOT) partnership developed capabilities to expose maritime data as a consumable Web-enabled service to authorized, unanticipated users employing community-based agreements defining a common vocabulary and data sharing services. This COI pilot also leveraged enterprise services resulting in a repeatable process, an extensible vocabulary, and reusable services available for developing responsive, agile solutions for any number of data sharing challenges.

The MDA DS COI pilot demonstrated the capability for three federal departments (DoD, DHS, and DoT) to share maritime vessel tracking data so that analysts and policing officials in all three departments will have the ability to exploit information they did not previously have. This mission is in direct response to objectives framed by the National Security Presidential Directive 41 and Homeland Security Presidential Directive 13 to improve maritime domain awareness of global threats to national and maritime security.

The MDA DS COI pilot also addressed information sharing objectives identified in the 2006 Quadrennial Defense Review (QDR), institutionalizing the ongoing transformation of the DoD. Specifically, it identified the approach taken to meet the National Defense Strategy requirement to enable net-centric operations. Section three of the document discussed the reorientation of capabilities and forces and identified actions to be taken to achieve net-centricity. That is, access to information, information sharing, and collaboration among those who need it. The QDR specifically requires the DoD to strengthen its data strategy.

The DoD Net-Centric Data Strategy establishes the policy approach to ensure information can be shared across the enterprise in a trusted and timely manner. Implementation is well under way. Today, it delivers capability as part of pilot initiatives developed by communities with specific information sharing needs. A net-centric COI develops capabilities to expose data as a consumable, Web-enabled service to *authorized unanticipated users employing community-based agreements defining a data sharing vocabulary and services*. The community-based agreements and their descriptions are published to discoverable registries where known and unanticipated authorized users may adopt or extend the agreements to meet additional mission-related data sharing requirements.

The MDA DS COI pilot addressed the cultural and technical challenges for multiple federal departments to come to agreements on how to improve awareness of potential security or defense related threats from maritime vessels, cargo, or crews. The cultural challenge focused on the need for data producers to share data with users with a right to use the data. This replaces the previous need-to-know paradigm that mitigated data being discovered and used by authorized unanticipated users. The cultural shift places a priority on trust and collaboration in a risk-managed data sharing environment. This is promoted by Executive Order 13388, directing improvements for sharing intelligence data and data sharing recommendations after the September 11th attack. Additionally, this effort faced the need for different federal departments to collaborate in defining their shared challenges, agree on a governance process to manage the effort, share resources needed (in the middle of a budget year without prior planning for this effort), come to agreement on a common vocabulary, and share lessons learned as the engineering teams developed the applications across four different data producer sites with different architectures. The key here is the COI was truly a community effort. The DoD Chief Information Officer (CIO) team met with each of the primary stakeholders to discuss the lack of visibility into data collected by other organizations and proposed the community-base approach to develop the vocabulary agreements and share in the engineering efforts. Each agreed this was a high priority problem and that the proposed COI-based process offered an opportunity to solve the problem relatively quickly. The DoD CIO team made recommendations based on an existing problem each COI participant already understood but had not come together to address before. Once the executive leadership determined this to be a priority effort and the staff understood the strategy, the effort was enthusiastically supported. DoD CIO team offered guidance as needed but did not lead the effort. The COI belonged to the community of organizations who would benefit from the effort. This commitment on the part of the COI members helped to ensure they understood the process and the benefits.

The technical challenge focused on moving from producer-to-user point-to-point interfaces, to producers posting data, services, and their descriptions to shared spaces that are discoverable and accessible by known and unanticipated authorized users. The value of networks and therefore collaboration increases as the number of participants increases. However, in the point-to-point design this becomes costly to manage and difficult to evolve. The use of shared spaces to host standard-based data assets and services scales in a more cost effective manner, meeting planned and unexpected mission needs. In addition to using shared spaces to offer data assets, a set of core enterprise services were made available as well. Offering the use of the DoD's Net-Centric Enterprise Services (NCES) Early Capability Baseline (ECB) release of enterprise services helped seal the agreements. Leveraging the NCES ECBs for security, messaging, and content discovery services meant the different

organizations did not have to reinvent these capabilities duplicating the cost, time, and risk. It also meant that all were interoperable and could use common interface standards. The key here is the pilot development and demonstration proved in real terms that reuse of enterprise services can work across technical and organizational domains.

The MDA DS COI was formed as a cross-functional and organizationally diverse community that was experiencing a data sharing problem. The COI defined the problem as a single statement and identified a limited number of data sources to expose as a consumable service for the initial pilot. The initial effort was scoped for a nine-to-12-month effort to rapidly develop the needed capability. The community adopted existing data standards in the development of semantic and structural agreements (extensible metadata schemas) to facilitate the understanding of the data by human or machine data users. Application-level services were developed using this community vocabulary to Web-enable legacy capabilities and commercial browsers to make the data visible and accessible in a trusted data sharing environment. Foundation level services adopted existing enterprise services from the DoD's NCES ECB, and the DHS's Homeland Security Information Network (HSIN). These enterprise services are designed for reuse across the respective enterprise, mitigating duplicative investments and reducing individual program risk, while enabling consistent performance similar to a public utility in the commercial sense.

The MDA DS COI documented the pilot effort as a repeatable process that resulted in successful demonstrations of the discovery and access to data from four functionally and geographically separate data producers within eight months. The repeatable process continues to evolve as it is shared with other COIs and in follow-on spirals for the MDA DS COI. The documented process and lessons learned are being consolidated and will be posted for additional use. The strategy is simple:

1. Define a data sharing problem among an operational community.
2. Gain leadership support and staff buy-in for the means of solving the problem as a community.
3. Develop the semantic and structural agreements for a common vocabulary all will agree on as the means of understanding and exchanging the data, (avoid selecting more than a dozen data sources to manage the risk and scope of the effort).
4. Adopt existing services as the technical means of sharing the data are developed.
5. Buy or create the services needed if no partial or complete services already exist.
6. Register the vocabulary and services in enterprise visible and accessible registries for follow-on use.
7. Demonstrate the working capability and market as a risk reduction for programs associated with sharing the same types of data, (this works even better if those programs participate in the pilot deriving direct benefit from the effort).
8. Document all of the lessons in the process for future use by this and other teams.
9. Post assets for general discovery, understanding, and use (vocabulary, services, repeatable process).

The execution of a successful pilot like this requires a strong, cooperative team and committed leadership support. This eight-month effort took between 60 and 90 days to develop the agreements on the problem set, resources needed, vocabulary and schema development, and the services needed. The development of Web-services leveraging the NCES ECBs and the HSIN became progressively easier, taking far less time with each subsequent implementation across the four data producer sites involved. Milestones were measured in days and weeks rather than months and years overall. As was stated before, the MDA DS COI team was enthusiastic in the pursuit of their goals sharing a clear understanding of the importance and benefits of working together as a team. Obstacles such as parochial ownership of needed assets were resolved quickly and the team was able to deliver.

The piloted capability demonstrated is available for limited use at this time. The pilot leveraged an early release of the NCES program that is under development. This in turn proved the value of the NCES effort to deliver a service-based infrastructure for reuse by DoD and other departments. As COIs apply the rapid development cycles and continue producing more user services and the NCES infrastructure adds more robust capabilities, this will be made available to a broader user community. Currently, the NCES program is approved for a limited operational support while developing at a rapid pace. The MDA DS COI and others are signing up to extend the initial success cited here implementing the Net-Centric Data Strategy and leveraging NCES (which increases the value of the NCES investment while reducing the cost to the DoD overall). Engineering lessons learned by the COIs are fed back into the NCES effort, providing further user guidance for the evolution of this enterprise program.

The demonstration allows a user to define their operational picture in near real time using live data feeds. The new MDA DS COI data sharing capability is a first step towards addressing the common challenge of global identification and tracking of maritime vessels, cargo, and crew using existing information sources to better secure our coasts, ports, and waterways. The successful eight-month pilot demonstrated proof of the DoD Net-Centric Data Strategy and implementation of an enterprise service-based architecture. COI members are studying means of applying the extensible data sharing capability in future spiral deliveries of operational programs supporting operational missions. The community is also exploring additional data sharing priorities to further improve global maritime domain awareness supporting the national defense and homeland security missions of the DoD, DHS, and DOT.

In a world where unforeseen human or natural disasters (i.e., U.S.S. Cole attack, September 11, Hurricane Katrina, and the 2004 Indian Ocean tsunami), may occur, this means of improving responsiveness and ability to develop solutions for data sharing needs is a critical solution for any number of data sharing challenges.◆

About the Author

Michael Todd is an advocate for the net-centric revolution across the DoD and its strategic partners. He is currently supporting DISA's NCES Program Office. His most recent accomplishment was to provide DoD CIO policy guidance and stewardship for the successful Maritime Domain Awareness Data Sharing Community of Interest pilot during 2006. Todd is a 1998 graduate of the Advanced Management Program at the National Defense University where he received his CIO and Information Resource Management Certifications.

DISA
ATTN: Mike Todd PEO-GES
PO Box 4502
Arlington, VA 22204-4502
Phone: (703) 882-0420
Fax: (703) 602-0830
E-mail: michael.todd@disa.mil

OFFICE OF THE CHIEF INFORMATION OFFICER,
US DEPARTMENT OF DEFENSE

The Power of
INFORMATION
Access Share Collaborate

Where it's needed, When it's needed, To those who need it most

Defense transformation hinges on the recognition that information is our greatest source of power. Information can be leveraged to allow decision makers at all levels to **make better decisions faster** and **act sooner**. Ensuring timely and trusted information is available where it is needed, when it is needed, and to those who need it most is at the heart of the capability needed to conduct **Network-Centric Operations (NCO)**.

Becoming Net Centric requires people, processes, and technology to work together to enable timely:
- **access** to information,
- **sharing** of information, and
- **collaboration** among those involved. Instead of "pushing information out" based on individually engineered and predetermined interfaces, Net-Centricity ensures that a user at any level can both "take what he needs" and "contribute what he knows."

The **Net-Centric Data Strategy** meets this challenge by focusing on data, rather than on the proprietary applications and programs that manipulate it (the current focus). Those at the source of the data will be required to make it easy to find and use. It must be:
- **visible**,
- **accessible**, and
- **understandable**.

Communities of Interest (COI) are collaborative groups of users who must have a shared vocabulary to exchange information. Data characteristics and content will be **"tagged"** in an agreed-to manner. The communities will range from pre-established groups with ongoing arrangements, to **Unanticipated Users** and non-traditional partnerships that develop on an ad hoc basis. Individual users will determine and display content based on their specific needs, **User Defined Operating Pictures (UDOPs)**, rather than in rigid or predetermined formats.

Information Assurance, the greatest Enterprise challenge, is the basis for trust: trust in the system's availability, the participants' identities, and the data's dependability and integrity. Today firewalls and software patches attempt to keep intruders out and data safe. Tomorrow's assured information will require that the individual data be secured throughout its useful lifespan.

The **Global Information Grid (GIG)** will enable Network-Centric Operations and collects, processes, stores and manages the Enterprise data. The GIG is not just a technological backbone. It includes:
- people,
- process, and
- technology.

The GIG enables "**information on demand**."

The **DoD Chief Information Officer (CIO)** provides the leadership to meet the Net-Centric vision and ultimately deliver the critical enabling capabilities required by the National Defense Strategy. Transforming to a Network-Centric Force requires fundamental changes in process, policy, and culture across the Department (defense operations, intelligence functions, and business processes).

The technological change will be significant, but the **cultural shift** may be even more challenging. The hallmark of the 21st century is **uncertainty**. Net-Centricity is rooted in a simple principle: **Confront uncertainty with agility**. To be agile, data can no longer be "owned"; it must be shared.

Timely and dependable information will be available across the Enterprise: from higher level headquarters and command centers, to a soldier in the city tracking insurgents, or a civilian in need of a new supplier. Ultimately, Net-Centricity means **Power to the Edge**.

Net-Centric Virtuosity

If you traveled through the L'Enfant Plaza Metrorail Station in Washington D.C, on January 12, 2007 between 7:51 and 8:32 a.m., you may – or may not – have witnessed a rare treat. A street musician – not an ordinary musician – Joshua Bell; recognized as the nation's best classical musician. He stood next to a garbage can in jeans, a long-sleeved t-shirt and a Nat's baseball cap and performed six pre-eminent classical pieces on a $3 million violin handcrafted in 1713 by Antonio Stradivari.

What many pay thousands of dollars to hear was free. *The Washington Post* arranged the performance as an experiment on context, perception, and priorities.

In 43 minutes, 1,097 people passed by the artist. Seven stopped for at least a minute, 27 gave money totaling $32.17, and 1,070 dashed by in oblivion. Gene Weingarten covered the event in a copious *Washington Post* article [1] including video clips on the *Post's* Web site [2].

The scene conjures up Churchill's observation, "Men occasionally stumble on the truth, but most of them pick themselves up and hurry off as if nothing had happened."

L'Enfant Plaza's coffee-toting, iPod-packing, serenity-scorning, deadline-chasing commuters resemble Net-centric's cell phone-toting, PowerPoint-packing, stovepipe-scorning, technology-chasing bureaucrats. Chances are they are one in the same: both justifiably busy, yet void of context, perspective, and priority. Still, within the crowds we find insight.

On his daily commute from Reston, John David Mortensen got off the escalator, located the violinist, checked the time, settled against a wall, and listened for three minutes.

"Whatever it was," he said, "it made me feel peace."

For the first time in his life, sensing something special, Mortensen gave money to a street musician. Net-centric stakeholders can learn from him. Amid the hustle, hype, and technical jargon take time to listen, dig below the surface, and confirm results before spending your money.

Sheron Parker and her son, Evan, walked past Joshua.

"There was a musician," Parker said, "and my son was intrigued. He wanted to pull over and listen, but I was rushed for time."

Stepping between her son and the musician, she exited. In fact, Weingarten reports, "Every single time a child walked past the musician, he or she tried to stop and watch. And every single time, a parent scooted the kid away."

Net-centric managers would be wise to listen and cultivate young engineers. Members of the first digital generation offer unsullied ears for technologies that work. Don't scoot them away.

A hundred feet away, J.T Tillman bought lottery tickets. He remembered every number he played but doesn't recall what the violinist played. When told he was one of the best musicians in the world, he laughed.

"Is he ever going to play around here again?"

Yes, J.T., but the price will be high to be within a hundred feet of Joshua Bell again. Despite what you hear on the trade show floor, there are no net-centric lotteries. Information technology history teaches us that those who don't exploit technology will pay a high price to the next Apple, Microsoft, or Oracle.

Calvin Myint passed four feet away from Bell but heard nothing over his iPod's pulsating ear-buds. Fixation on a technology can limit our exposure to new possibilities, experiences and insights. Even horse blinders were state-of-the-art once.

George Tindley was bussing tables at a coffee shop across from the station. He listened to Bell's playing at the edge of the shop.

"You could tell in one second that this guy was good," Tindley said, "Most people, they play music; they don't feel it ... that man was feeling it."

Remember your net-centric client – the warrior. They need the right information at the right time, but more importantly, they need to feel the context of the information.

Bell, the virtuoso himself, was actually nervous.

"When you play for ticket-holders," Bell explains, "you are already validated. Here, what if they don't like me? What if they resent my presence…?"

Joshua's musical talent is best appreciated in the optimal conditions of the world's best concert halls. His music could have lost context within the chaos of the metro station. Likewise, information can lose context in the fog of war. Net-centric focus should be more than interoperability, ready access, and massive data. The tip of the net-centric spear is a warrior with optimal viewing conditions.

Louis Pasteur lamented, "In the field of observation, chance favors the prepared mind."

— Gary A. Petersen
Arrowpoint Solutions
gpetersen@arrowpoint.us

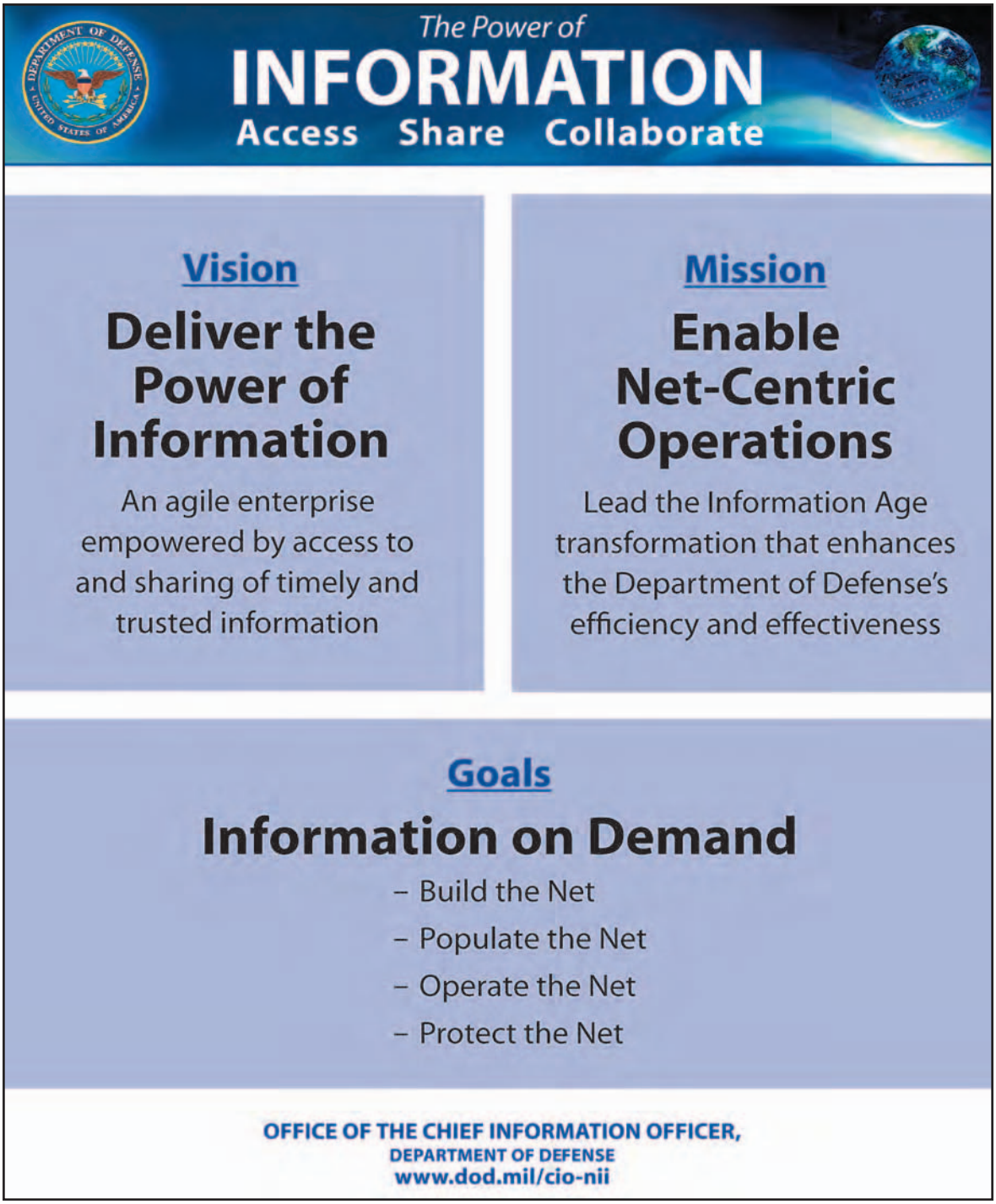
References

1. Weingarten, Gene. "Pearls Before Breakfast." Washington Post 8 Apr. 2007: W10.
2. Washington Post <www.washingtonpost.com/wpdyn/content/article/2007/04/04/AR2007040401721.html>.

Can You BACKTALK?

Here is your chance to make your point, even if it is a bit tongue-in-cheek, without your boss censoring your writing. In addition to accepting articles that relate to software engineering for publication in CROSSTALK, we also accept articles for the BACKTALK column. BACKTALK articles should provide a concise, clever, humorous, and insightful perspective on the software engineering profession or industry or a portion of it. Your BACKTALK article should be entertaining and clever or original in concept, design, or delivery. The length should not exceed 750 words.

For a complete author's packet detailing how to submit your BACKTALK article, visit our Web site at <www.stsc.hill.af.mil>.



CrossTalk / 517 SMXS/MXDEA
6022 Fir AVE
BLDG 1238
Hill AFB, UT 84056-5820

PRSRT STD
U.S. POSTAGE PAID
Albuquerque, NM
Permit 737